To appear in P. Markopoulos, B. de Ruyter and W. Mackay, eds.: Awareness Systems: Advances in Theory, Methodology and Design. Berlin, Heidelberg: Springer Verlag.

Privacy Considerations in Awareness Systems: Designing with Privacy in Mind

Sameer Patil and Alfred Kobsa

1 Introduction

The earlier chapters of this book present a conceptual understanding of awareness [28, 54]. A historical account [70] as well as descriptions of various implementations (see Section III of this book) illustrate how various systems have attempted to foster greater awareness. A common challenge faced by all awareness systems is the tension with an individual's desire for privacy [39].

Interaction between awareness and privacy is not limited to awareness systems but is a characteristic of everyday life. As Schwartz [73] notes, "We are led to relinquish our private information and activities by the expediencies and reciprocities routinely called for in daily life. We all know, for example, that in order to employ others as resources it is necessary to reveal to them something of ourselves".

In the case of awareness systems, the benefits for the recipients of information typically come at the cost of the risks of reduced privacy for the individuals whose information is disseminated. Moreover, these systems require users to extend their existing practices regarding awareness and privacy, from the familiar physical domain to the newer digital domain. Situations that lack of familiarity are known to be problematic for privacy management though, and may lead to privacy violations [71].

Privacy management in the digital domain poses precisely such difficulties. Certain characteristics of the digital domain differ substantially from the physical world, namely, high-speed transmission, potential persistence, and enhanced computation of information. The digital domain may also result in disembodiment [36] (e.g., one may be represented only by a screen name). Disembodiment thwarts the ability to exploit the rich cues that are readily used in face-to-face interactions (e.g., posture,

Sameer Patil
Department of Informatics, University of California, Irvine, e-mail: patil@uci.edu

Alfred Kobsa
Department of Informatics, University of California, Irvine e-mail: kobsa@uci.edu

expressions, intonation). In addition, dissociation of interaction [13] could occur when only the results of people's actions are shared while the actions themselves are not visible (e.g., a Wiki page with no version history available). Owing to these differences, the transformation of expectations and behaviors from the physical to the digital world is not always effective, or even possible.

As a result, designers of awareness systems face the significant challenge of satisfying users' awareness as well as privacy needs simultaneously. Insufficient attention to either of these needs has the potential to undermine the usage of the system. When the users are unable to achieve appropriate levels of awareness and privacy without great effort, they may not exploit the system's potential fully. For instance, Lee et al. [50] found that when privacy was desired, users of their Portholes video system preferred to turn their cameras off since fiddling with other privacy options, such as blurring the video, was too cumbersome. Similarly, Herbsleb et al. [37] found it difficult to attain substantial usage of their chat system because its default settings were too private. The system imposed significant initial setup efforts on its users before it could provide any awareness benefits. Likewise, in our own research we found that users who were forced to use instant messaging (IM) due to organizational requirements often resorted to circumvention tactics. For instance, some set their status to "away" or "busy" even when they were not, or conversely, some changed their preferences so as to appear online even when they were away from their desks [64, 65]. Such underuse or circumvention results in suboptimal use of awareness systems.

Focusing on awareness without paying sufficient attention to privacy aspects may evoke strong user backlash. A recent example that involves the social networking site Facebook (http://www.facebook.com) is a poignant reminder. Facebook introduced a new awareness feature that automatically presented to each user an aggregation of every single activity of their friends. Tens of thousands of users were outraged because they felt that such automatic broadcast a great violation of their privacy. The revolt ranged from online petitions and protest groups to threats of a boycott [18]. This episode underscores that user opposition due to privacy concerns can translate into minimal use or even the abandonment of the system. If this happens, organizations stand to lose their investments in deployed awareness applications. Moreover, the companies that design and build these systems, as well as their customers, face the prospect of longer-term damage to their trust and credibility in the users' eyes [4, 5].

Thus, it is important for awareness systems to respect the privacy concerns of their users. This chapter analyzes theoretical and empirical work in order to aid designers in building privacy-sensitive awareness systems.

2 Privacy

The notion of privacy has recently received enormous attention both in the scientific literature and in the popular press. Figure 1 shows the number of non-fiction books

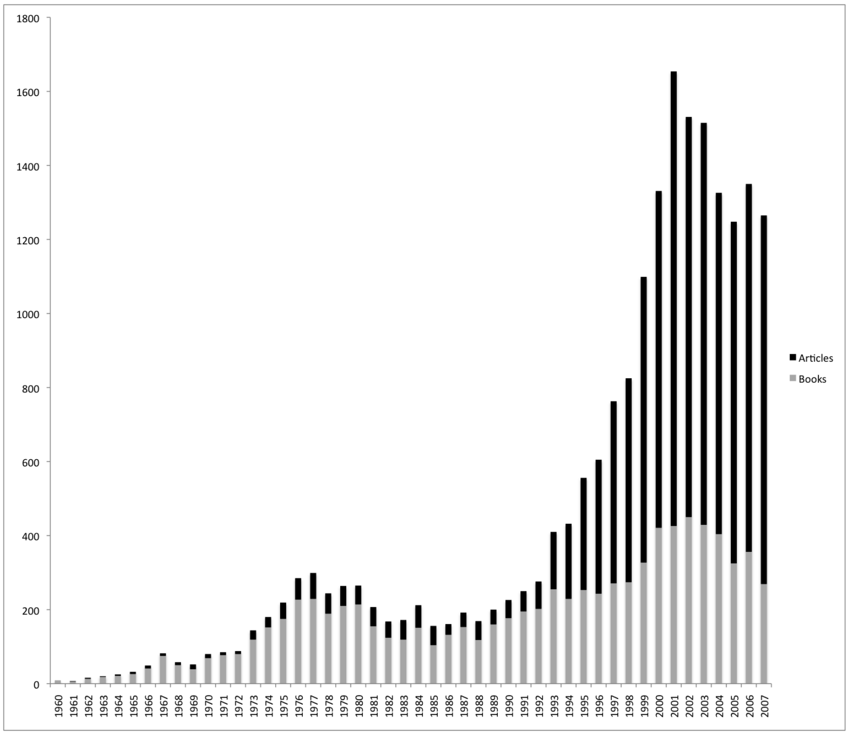

Fig. 1 WorldCat non-fiction books and articles with ”privacy” in title

and articles with “privacy” in their titles that have been published since 1960[1]. Of the about 21,000 publications, nearly two-thirds have been published in the past ten years alone. This dramatic rise in the research productivity from the mid-1990s onwards coincides with the advent of the World Wide Web and e-Commerce. The small peak in the 1970s corresponds with the global induction of data processing into businesses and government administration. (Both of these changes engendered widespread privacy concerns, and led to privacy legislation in some parts of the world). To some extent, the rapid increase of research articles as opposed to books mirrors the scientific disciplines in which privacy research takes place. While privacy research originated in the fields of law, psychology, sociology, communications, political science, architecture and urban design, it has since expanded into the computer and information sciences, organization and management research, economics, and the health sciences.

The concept of privacy is so intricate that there is no universal definition of it. The difficulty of defining privacy stems from its highly situated [75] and context-

[1] The data were obtained through a search in WorldCat, the world’s largest library network with 1.2 billion items from the catalogues of more than 10,000 libraries worldwide. Duplicates have been removed from the retrieved results.

dependent nature. Even in the same situation, different individuals may have differing opinions and expectations regarding what privacy means to them (for example, based upon stated preferences, Westin [79] classified individuals as privacy fundamentalists, pragmatists, or unconcerned). This context dependency and variability between individuals make dealing with privacy a difficult task. To quote Lederer et al. [46]:

> "One possible reason why designing privacy-sensitive systems is so difficult is that, by refusing to render its meaning plain and knowable, privacy simply lives up to its name. Rather than exposing an unambiguous public representation for all to see and comprehend, it cloaks itself behind an assortment of meanings, presenting different interpretations to different people".

There are three main perspectives from which the notions of privacy are commonly described and analyzed (see Table 1):

Table 1 Three perspectives regarding the concept of privacy

Perspective	Concept of Privacy	Enacted by	Consequences of Privacy Violation
Normative	Right or freedom	Laws, Contracts, Policies	Civil and/or criminal penalties
Social	Socially constructed	Individual and collective everyday social action	Potential embarrassment or breakdown in relationship(s) etc.
Technical	Control over data and information	Automated and/or manual access control	Identity theft, Unauthorized access, Illegal use of information

Normative:

Analyzed philosophically, privacy is an ethical concept [58, 41, 53]. Privacy is viewed as a "right" of individuals, and, thus, as a matter of "freedom". For example, Warren and Brandeis [77] characterized privacy as "the freedom to be left alone". From this perspective, privacy is a civil liberty that needs to be protected through legal and political means. Traditionally, the focus of privacy protection has been on laws, contracts and policies aimed at protecting the individual from large entities such as corporations and governments [51]. Increasingly, however, legislation is being extended to protecting one's privacy from other individuals (for instance, laws against hacking, stalking or voyeurism).

Social:

From the social perspective, privacy has psychological and cultural roots [78, 73]. Privacy is "socially constructed" based on the behavior and the interactions of individuals as they conduct their day-to-day affairs. For instance, in Goffman's [33] analysis "the expressive component of social life has been treated as a source of impressions given to or taken by others", where expression "has been treated in terms of the communicative role it plays during social interaction". This manifests itself in Rachels' [69] claim that "privacy is necessary if we are to maintain the variety of social relationships with other people that we want to have". Thus, managing privacy allows us to manage social relationships. Altman [7] has described the process of privacy management as a "dialectic and dynamic boundary regulation process" – conditioned by the expectations and experiences of the parties involved and under continuous negotiation and refinement. Given the differences in norms, expectations, experiences, behaviors, and laws across cultures, it is no surprise that privacy manifests itself differently in different cultures [78, 55]. Viewed socially, the notion of privacy evolves as external changes bring about changes in expectations and behavior, or as technology introduces new forms or means of interaction.

Technical:

The technical perspective views privacy in terms of the functional characteristics of digital systems. Discussions from this perspective tend to investigate how ethical and social considerations could be operationalized. Privacy is thus treated as the desire for selective and adequate control over data and information – both incoming and outgoing. For example, Stone et al. [74] describe privacy as the "ability of the individual to personally control information about oneself" whereas Samarajiva [72] extends it to the "control of outflow of information that may be of strategic or aesthetic value to the person and control of inflow of information including initiation of contact". The issues under consideration include the capture, storage, ownership, usage, and access of personal data. For instance, the code of Fair Information Practices was developed from this perspective [76].

To summarize, the social perspective focuses on what practices relate to privacy, while the normative discussions look at whether a particular behavior is ethically (or legally) justified. The technical discourse is concerned with how the ethical and social understandings can be represented formally, and implemented practically in an operational system. The three perspectives are not mutually exclusive but interdependent. Privacy laws may be enacted based on technical or social considerations, while social interactions may be altered due to changing laws and technology.

Having laid out the foundational understandings of privacy, we now proceed to discussing how awareness and privacy interact with each other.

3 Relationship between Awareness and Privacy

Given that the concepts of awareness and privacy are both related to disclosure, it should not be surprising that the two interact with each other. This interaction between awareness and privacy is not new. Westin [78] describes it as a balancing act:

> "Privacy is neither a self-sufficient state nor an end in itself, even for the hermit and the recluse. It is basically an instrument for achieving individual goals of self-realization. As such, it is only part of the individual's complex and shifting system of social needs, part of the way he adjusts his emotional mechanisms to the barrage of personal and social stimuli that he encounters in daily life. Individuals have needs for disclosure and companionship every bit as important as their needs for privacy. As ancient and modern philosophers agree, man is a social animal, a grebegarious being whose need for affiliation marks his conduct in every society. Thus, at one hour a person may want lively companionship and group affiliation; at another moment, the intimacy of family or close friends; at another the anonymity of the city street or the movie; at still other times, to be totally alone and unobserved. To be left in privacy when one wants companionship is as uncomfortable as the inability to have privacy when one craves it.
>
> [. . .] All individuals are constantly engaged in an attempt to find sufficient privacy to serve their general social roles as well as their individual needs of the moment. Either too much or too little privacy can create imbalances which seriously jeopardize the individual's well-being."

In the context of awareness systems, this equilibrium corresponds to a reconciliation of the benefits of awareness for improving effectiveness and efficiency, and the potential risks of reduced privacy.

In the physical setting of everyday life, individuals utilize the spatial and architectural features of the environment [73] (e.g., a door), the biological and cognitive features of humans [78] (e.g., limitations of human memory), and the shared understanding of norms [78] to meet their awareness and privacy needs. Thus, situations in which one's familiarity with the aspects of day-to-day affairs breaks down (e.g., moving to a foreign country) have been observed to be problematic for privacy management.

Privacy is managed based on one's familiarity with these features and the understanding of norms, acquired through daily life experiences. This, of course, does not imply that privacy violations could never occur in familiar everyday settings. In fact, privacy violations due to accidental disclosure are not uncommon [73]. When a violation of privacy does occur, and is detected, individuals typically engage in social negotiation until a commonly agreed upon (or comfortable) state of privacy is reached for everyone involved. Westin [78] describes practices such as covering one's face, averting others' eyes, or facing the wall. As Palen and Dourish [63] point out, "Privacy is understood to be under continuous negotiation and management, with the boundary that distinguishes privacy and publicity refined according to circumstance".

Recent technological developments, e.g., in the fields of Computer Supported Collaborative Work (CSCW), have introduced the digital domain as an additional arena in which awareness and privacy need to be reconciled [6]. The next subsection describes how the digital domain, due to its relative novelty and its unique characteristics, poses new challenges in this regard.

3.1 Digital Domain

We noted earlier that situations in which familiarity breaks down are problematic for privacy management, and could lead to privacy violations. Awareness systems create exactly such problems since they require users to extend their privacy management practices from the familiar physical domain to the relatively new digital domain.

Additionally, certain characteristics that distinguish the digital domain from the physical world are important from a privacy standpoint. Salient among these are:

Transmission:

The ease, speed, and low cost with which data is transmitted in the digital domain are major reasons why it is attractive for fostering awareness. However, these advantages come at the expense of increased risk for unauthorized access through technical means such as hacking and network sniffing, and higher potential damages that may result from such attacks.

Persistence:

Due to the availability of practically infinite storage capacity, the digital domain increases the temporal dimension of data indefinitely. In contrast, information about the vast majority of routine activities in the non-digital world could be trusted to be merely ephemeral. The digital "trails" of one's activities undermine the "plausible deniability" [56] of facts and actions that one may not want to admit to. It also separates information from the context in which it was generated [23]. Moreover, the storage of personally identifiable information introduces legal issues of accountability, liability etc. For example, a Chinese journalist was convicted of leaking state secrets based on records of his Internet activities provided by Yahoo! Inc. [42].

Computing power:

Data in the digital form is amenable to the kinds of analysis that are almost impossible in a non-digital format. Additionally, computing power makes it possible to automate such analyses. For example, techniques like data mining, pattern detection, social network analysis, event notification, visualization etc. can be used for inference, prediction, profiling, surveillance, and much more.

Disembodiment and dissociation:

As mentioned earlier, interactions between individuals mediated by the digital domain can suffer from disembodiment [36] and dissociation [13]. Disembodiment and dissociation hinder one's ability to present oneself as effectively to others as in a face-to-face setting, and result in a breakdown of social and behavioral norms and practices [13]. For example, Goffman [33] describes how people present different appropriate "faces" in real life quite seamlessly. Yet, a direct operationalization of this metaphor in a digital system turned out to be unsuccessful [49]. Moreover, disembodiment could result in individuals being forced to be explicit about certain information that is otherwise intuitive or implicit [13].

As a result of these distinctions, the digital domain can inhibit behaviors that may be fluid and seamless in the social realm. Thus, privacy runs into what Ackerman [1] characterizes as the social-technical gap, i.e., "the divide between what we know we must support socially and what we can support technically" . On the other hand, characteristics of the digital domain enable actions that may otherwise be impossible or prohibitively difficult to achieve socially. Lessig [51] sums this up rather nicely:

> "In the 1790s the technology was humans; now it is machines. Then the technology noticed only what was different; now it notices any transaction. Then the default was that searchable records were not collected; now the default is that all monitoring produces searchable records. These differences add up."

4 Relevant Research

Over the past few years, the importance of taking action on privacy issues engendered by awareness systems has gained increased attention. Research that tackles privacy in awareness systems falls along three major themes: users studies of specific awareness systems, design principles and guidelines derived from theoretical considerations, and privacy-enhancing technical solutions. We discuss each of these below.

4.1 User Studies

Initial findings related to privacy were primarily noted "on the side" in studies aimed at evaluating experiences with the awareness aspects of systems. Dourish [24] characterizes privacy controls along a "social-technical continuum". On the social end of this continuum, social pressures and norms are relied upon to prevent system abuse, while on its technical end, technology prevents attempted misuse. Social controls are likely to work well within small and relatively well-knit communities only [24, 3]. Even in such environments with high levels of interpersonal trust, social controls may result in very strong protective behaviors such as turning the system off or altering ones work habits [52]. In contrast, technical privacy protections raise the acceptance and adoption of a system by virtue of the fact that it increases user trust that the system would protect privacy [24]. Later studies confirm that trust in a system is an important implicit factor in privacy assessments [4, 5, 67].

Palen [62] found that socio-technical mechanisms controlled privacy even in highly open network calendaring environments. Users managed privacy partly via technical access control, partly via the norm of reciprocity [2], partly via practices such as cryptic entries, omissions, defensive scheduling, and partly via social anonymity within the larger organizational context. Lee et al. [50] suggest that mere existence of mechanisms to address privacy needs is not enough; these mechanisms need to be lightweight. In other words, users desire mechanisms that allow them "to increase or decrease privacy, to inform other users of their new privacy state and to provide immediate feedback of the change, in a way that "facilitates the tight coupling between the means to change privacy and the means to obtain feedback that privacy is attained". As Herbsleb et al. [37] discovered, the lack of lightweight, low-burden privacy management mechanisms increased setup time. Moreover, Grinter and Palen [34] illustrate (albeit with teenagers) that users adapt system capabilities to their own ends. Teens in their study made enterprising use of access permissions, profiles, status messages and screen names to manage privacy. Additionally, Nardi et al. [56] noticed that plausible deniability of physical presence was used frequently by IM users as a means for privacy management.

Recently, studies of awareness systems have started targeting privacy as the primary object of investigation. These studies have unveiled a number of factors that affect users privacy judgments. These include users relationship with the information recipient, the purpose and usage of requested information, the context, and the sensitivity of content [4, 5, 48, 64, 19, 60]. Lederer et al. [49] also showed that a-priori manual configuration of privacy preferences is better than automatic strategies – especially for information that users deem important.

Generic privacy attitudes and behaviors could also come into consideration in awareness systems. Therefore, it is instructive to look at a few privacy studies conducted in other contexts. For instance, as mentioned above, Westin [79] classified individuals into three main clusters – privacy fundamentalists, pragmatists, and unconcerned. This distinction may also apply to privacy concerns in the context of awareness systems. Milberg et al. [55] and Bellman et al. [11] reported that privacy concern varies by country. At the same time, they mentioned that "secondary use" and "improper access" rank as the top two concerns across most nationalities. Cranor et al. [20] listed anonymity and information sensitivity as important privacy-related factors for Internet users. Finally, Fox [30] showed that users are often ignorant of the basic concepts underlying their digital domain activities, and do not typically utilize the tools available for privacy protection.

[2] Palen [62] found that individuals with unusually restrictive, or liberal, calendar access settings often had immediate colleagues with similar access configurations.

4.2 Theories, Principles and Guidelines

Privacy is recognized to be a nuanced and situated concept that escapes universal definition. The rich body of literature on privacy in the social sciences is testimony to its intricate connections with the broader social context [25]. Owing to this complexity, technology designers have found it difficult to translate the privacy-related findings of the various user studies into concrete system design guidance. Researchers have tried to address this problem by framing the theoretical insights into privacy in forms that are more amenable to system designers. For instance, Boyle and Greenberg [16] describe a vocabulary of privacy that permits designers to discuss privacy in an unambiguous manner. To suggest ways of thinking about privacy in socio-technical environments, Palen and Dourish [63] outline a model of privacy that is based on the theory developed by social psychologist Irwin Altman [7, 8]. It characterizes privacy as a process that regulates the boundaries of disclosure, identity and temporality. This process is both dynamic (i.e., shaped by personal and collective experiences and expectations) and dialectic (i.e., under continuous boundary negotiation).

Researchers in the technology trenches have further distilled general guidance on privacy into specific design principles and guidelines in order to enable better privacy management. Bellotti and Sellen [14] propose a design framework based on feedback and control regarding information capture, construction, accessibility, and purpose. TIn essence, feedback mechanisms aim at providing users with information that helps them make privacy judgments, and control mechanisms empower them to take appropriate actions to manage privacy. In addition, Bellotti and Sellen [14] provide eleven criteria for evaluating design solutions – trustworthiness, appropriate timing, perceptibility, unobtrusiveness, minimal intrusiveness, fail-safety, flexibility, low effort, meaningfulness, learnability, and low cost. Langheinrich [44] draws upon Fair Information Practices [76] in proposing that privacy-sensitive systems ought to notify the user appropriately, seek consent, provide choice, allow anonymity or pseudonomity, limit scope with proximity as well as locality, ensure adequate security, and implement appropriate information access. Iachello and Abowd [40] add the principle of proportionality – "any application, system tool, or process should balance its utility with the rights to privacy of the involved individuals". In contrast, Lederer et al. [46] outline five pitfalls – obscuring potential information flow, obscuring actual information flow, emphasizing configuration over action, lacking coarse-grained control, and inhibiting existing practice. Hong et al. [38] further develop privacy risk models to analyze how well a system meets such principles or avoids the pitfalls. These risk models are a set of information sharing questions pertaining to the social and organizational context in which the system is situated, and the technology which is used to implement the system. Finally, to incorporate user perceptions, Adams and Sasse [5] provide a privacy model based on interacting concerns information sensitivity, information receiver and information usage.

4.3 Design Techniques

Incorporating the principles and guidelines into working systems continues to pose challenges for designers. Improving privacy management requires addressing multiple conflicting concerns simultaneously [Hudson and Smith 1996], such as privacy vs. awareness, risks vs. benefits, control vs. overhead, and feedback vs. disruption. To complicate matters further, an acceptable solution to these tradeoffs is highly dependent on the user as well as the context.

Several techniques have been proposed and explored for the implementation of such principles. These include:

- encryption [22];
- access control via preferences, policies, and roles [27, 80];
- mechanisms to reduce the burden of preference specification such as lightweight interfaces [45], or grouping and templates [60, 67];
- automatic or manual control of the granularity of disclosed information [26, 50, 62, 19];
- feedback via visualization [35], sound [32], intelligent agents [2], and contextual disclosure [43];
- distortion of disclosed information [15];
- support for anonymity (or pseudonymity) [9];
- inference of appropriate awareness disclosure based on modeling [10].

Describing these techniques is beyond the scope of this chapter. The reader is referred to the cited works for details. In practice, no technique alone can satisfy all requirements and constraints. A typical awareness system would likely combine multiple privacy management approaches.

5 Positioning Awareness Systems

In order to choose the most relevant insights from prior work, we propose that a given awareness system be positioned in a space of three independent dimensions (see Figure 2). We discuss these dimensions below.

5.1 Nature of Awareness Mechanisms

By their very nature, all awareness systems deal with capturing, storing, analyzing, disseminating, and/or displaying awareness information in some form. However, there is a distinction to be made between systems that are built specifically for awareness purposes (e.g., [26, 9, 17]), and those that provide awareness implicitly by virtue of their use [12]. For instance, the primary purpose of email is to communicate the content of a message. Yet, by virtue of the timestamp, IP address, server

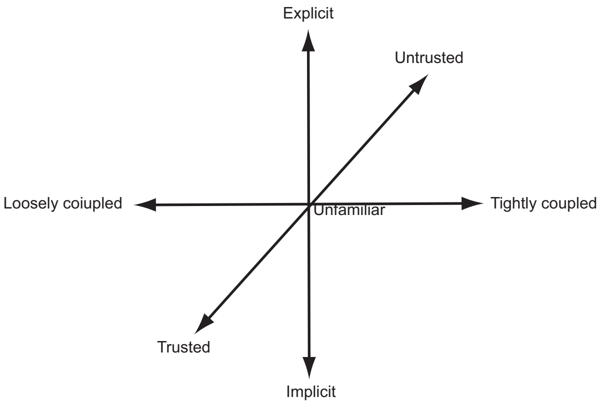

Fig. 2 Positioning awareness systems along privacy-relevant dimensions

names and other header information, email reveals additional information implicitly. (It is also important to note that researchers have been exploring systems that could be built on top of other systems to make implicit aspects of awareness more explicit [29, 31].) Thus, awareness systems can be characterized to lie along a continuum ranging from explicit to implicit awareness functionalities (see Figure 2). For example, a system like Instant Messaging (IM) that provides communication mechanisms along with awareness [56] could be positioned somewhere in the upper half.

Systems that deal with awareness information explicitly, try to expose the benefits of awareness in a direct manner. As a result, they may also draw direct attention to the associated privacy issues. In contrast, when awareness is implicit or secondary to the function of a system, the primary attention of the user is on other aspects of the task carried out with the system (e.g., the user is much more likely to focus on the contents of an email message rather than on the IP address from which the email is being sent). Consequently, the privacy aspects remain invisible in such cases [12].

5.2 Activity Coupling

The user activities that awareness systems support lie along a continuum from loosely to tightly coupled [61, 59, 57]. For instance, the work of software developers working on two separate modules of the same program may be less tightly coupled than that of a developer and a tester working on the same module.

As Olson and Olson [59] explained, tightly coupled activities typically require "frequent, complex communication among the group members, with short feedback loops and multiple streams of information". Therefore, when the work is tightly coupled, the awareness among collaborators of each other's activities is automatically improved as a side effect of more frequent and prolonged interactions. Given the shared (and often synchronous) focus on the same activity, awareness functionalities in these circumstances are mainly concerned with ensuring that the parties involved are aware of the focus and understanding of others [26]. On the other hand, when collaborative activities are loosely coupled, awareness is impoverished. In such cases, a variety of factors may affect awareness unfavorably. These include less frequent and asynchronous interaction between collaborators, less shared context, and involvement of the collaborators in multiple simultaneous tasks and projects [61, 68]. Thus, the looser the coupling, the greater is the need for external support by awareness systems.

Similarly, the privacy expectations in loosely coupled distributed activities can be expected to be greater than in the case of tightly coupled work. This may be caused by the same factors that engender impoverishment of awareness (i.e., less frequent and asynchronous interaction, less shared context, multi-tasking etc.) Additionally, if the work is geographically distributed across different countries, different privacy attitudes and laws of different nationalities may need to be considered [55, 11]. In contrast, tightly coupled activities involve more focused (and often synchronous as well as co-located) interactions that allow one to monitor privacy closely.

5.3 Nature of Relationships

The nature of the relationships among various users of an awareness system forms the third dimension. These relationships can range from trusted and familiar (e.g., a colleague with whom one shares an office) to unfamiliar (but known, e.g. an employee in a different branch of the organization) to untrusted (e.g., a stranger who might read one's blog). The degree of familiarity with the individual with whom one interacts is important in shaping attitudes and behaviors. For instance, greater familiarity reduces the importance of static awareness information [21] because collaborators are likely to already know it, or could ask for it directly [47]. Lederer et al. [47] point out differences in privacy considerations when dealing with familiar as opposed to unfamiliar parties. While a great deal of research and legislation focuses on privacy protection from organizations and unknown people (e.g., governments, corporations, hackers, stalkers, marketers), the other side of the continuum has received lesser attention. Yet, this side – ranging from the trusted to the unfamiliar – is of greater importance when dealing with awareness systems.

6 Designing with Privacy in Mind

Designers can utilize the above work of others to tackle privacy issues in their own awareness systems. Yet, we believe that in order to improve the privacy-sensitivity of awareness systems, a focus on privacy is needed right from the earliest conceptual phases of system development. As the term "awareness system" implies, the purpose of the system is to foster awareness. Hence, system designers have so far focused on providing awareness while privacy has only received secondary attention. We urge designers to treat privacy on an equal footing with awareness when building systems. The abovementioned principle of proportionality [40] is a step in that direction. However, it deals mainly with a cost-benefit analysis of awareness and privacy to decide whether or not a system should be built at all. We take one step further and advocate that even after using this principle at the beginning of the design process to decide that an awareness system should be built, designers must continue to consider privacy at every subsequent step in the design cycle.

Two examples from our own research – one positive and one negative – illustrate why it is essential to keep privacy in mind at all stages of system development.

6.1 Workplace Awareness Application

We designed an awareness application called mySpace to support the collaborative work of knowledge workers who were co-located in the same building [67]. The mySpace application is a browser-based interactive visualization of a user's physical workplace that provides dynamically updated information about people, places and equipment. Recognizing that mySpace would lead to privacy concerns, we sought to empower the users to manage their privacy according to their own preferences. Our initial intuition (based on the experience with the organizational culture) was to allow users to specify one set of preference for their immediate team, and another set for all others. Additionally, we wanted to make the operation of the system transparent for users by disclosing all pieces of individual information to which mySpace had access. Yet, we feared that doing so would scare users into selecting more privacy-protective preferences, thereby undermining the awareness benefits.

Instead of proceeding to build the system as envisioned, we conducted a user study of an early prototype. To our surprise, we found that our intuition was not aligned with the users' desires. Users wanted to manage privacy at a finer grain by specifying preferences differently for multiple groups of contacts. Also, increased system transparency promoted trust in the system and seemed to reassure users that the system would honor their preferences. This resulted in increased awareness being provided to close, trusted groups of contacts. Studying how users deal with privacy aspects at the prototype stage allowed mySpace to be sensitive to the practices of its target population. It also spared the costs and difficulties of correcting privacy management mechanisms retroactively after deployment.

6.2 Instant Messaging Privacy Plugin

Our experiences gained from attempting to improve the privacy management in existing IM systems illustrate the weaknesses of the retrofitting approach. Based on

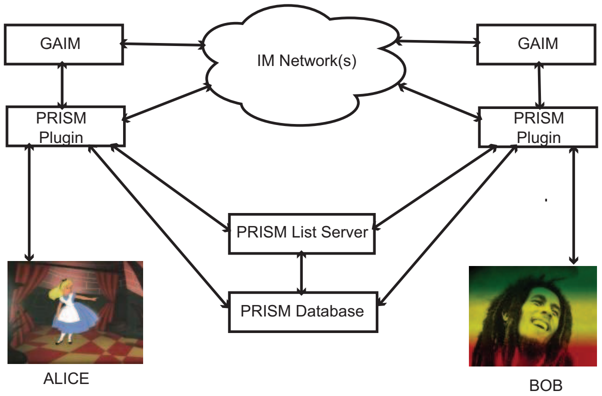

Fig. 3 System architecture for PRISM

several interviews and a survey of IM users [64, 66], we had identified several avenues for improving IM privacy management. However, not having access to the servers of the commercial IM networks made the task of implementing our improvements challenging. We thus packaged our privacy management extensions as a plugin for the open source multiple IM client GAIM (now Pidgin). The plugin is called PRISM (for PRivacy-Sensitive Messaging). The architecture of the enhanced IM system is shown in Figure 3.

As can be seen, it was necessary to maintain a separate server and a database in order to provide some of the privacy extensions. One enhancement that PRISM provides is to allow users to view the IM activities of others at a group level in order to facilitate a comparison with one's own activities. The database logs various IM actions of interest, such as when users log in, log off, or change their availability status. Since PRISM does not have access to the servers of the IM networks, such logging is essential for generating the visualizations of the activities. Ideally, the servers of the IM network would need to be extended to incorporate these functions.

More significantly, we often ran into limitations imposed by the specifics of the IM protocol(s). For instance, we aimed at empowering users to specify their privacy preferences differently for different groups of contacts. However, the IM protocol(s) lacked sufficient nuance to achieve this for all settings. For example, we were able to allow users to specify a different status for different groups but unable to provide a way to specify that only certain groups could view the length of time they were idle. Such deficiencies reflect inadequate attention to user privacy practices during the development of the IM protocol(s).

Finally, we aimed building privacy enhancements that were generic such that they did not rely on the specifics of any single IM system. However, ensuring such common cross-IM experience is a challenging task because IM systems differ in the details of their protocols, and of their server implementations. For example, some IM systems allow one to broadcast the length of the user's idle time, others don't; some IM systems allow multiple simultaneous logins, others don't. We found that catering to the lowest common denominator limits the extent to which the IM client can add, or improve upon, privacy management features. The only remaining option is to treat each protocol differently. This approach may confuse users because the privacy management experience and expectations are no longer uniform.

Overall, PRISM serves as a cautionary example and illustrates the challenges and difficulties that designers are likely to face when attempting to retrofit privacy enhancements rather than designing systems with privacy in mind right from the outset.

7 Conclusion

Handling user privacy appropriately is a significant challenge for awareness systems. Inadequate attention to privacy issues may be a barrier to their success. To build awareness systems that are sensitive to the privacy needs of their users, designers ought to pay attention to privacy at every stage of system design. In order to be effective in this task, designers need to be aware of the various ways in which privacy can be understood. They should also pay attention to the special characteristics of the digital domain that may affect privacy management. Fortunately, designers can draw upon a substantial body of insights regarding privacy in the research literature. Appropriate techniques need to be chosen based on a careful evaluation of the context of the work activities and the social relationships within which the awareness system under consideration operates. Designing awareness systems with privacy in mind has the potential to enhance privacy sensitivity significantly, and to empower users to satisfy their awareness as well as privacy needs optimally.

Acknowledgements Some of the research described was supported by NSF Grant No. 0205724. We wish to acknowledge our collaborator Jennifer Lai. We also wish to thank the subjects who participated in our study on mySpace. Finally, we are grateful to Mihir Mahajan for helping proofread various drafts of this chapter.

References

1. Ackerman, M.S.: The Intellectual Challenge of CSCW: The Gap between Social Requirements and Technical Feasibility. Human-Computer Interaction **15**, 179–203 (2000)
2. Ackerman, M.S., Cranor, L.: Privacy Critics: UI Components to Safeguard Users' Privacy. In: CHI '99: CHI '99 Extended Abstracts on Human Factors in Computing Systems, pp. 258–259. ACM, New York, NY, USA (1999). DOI http://doi.acm.org/10.1145/632716.632875
3. Ackerman, M.S., Starr, B., Hindus, D., Mainwaring, S.D.: Hanging on the 'Wire: A Field Study of an Audio-only Media Space. ACM Trans. Computer-Human Interaction **4**(1), 39–66 (1997). DOI http://doi.acm.org/10.1145/244754.244756
4. Adams, A.: Users' Perception of Privacy in Multimedia Communication. In: CHI '99: CHI '99 Extended Abstracts on Human Factors in Computing Systems, pp. 53–54. ACM, New York, NY, USA (1999). DOI http://doi.acm.org/10.1145/632716.632752

5. Adams, A., Sasse, M.A.: Privacy Issues in Ubiquitous Multimedia Environments: Wake Sleeping Dogs, or Let Them Lie? In: Seventh IFIP Conference on Human-Computer Interaction INTERACT'99, pp. 214–221 (1999)
6. Agre, P.E., Rotenberg, M. (eds.): Technology and Privacy: The New Landscape. MIT Press, Cambridge, MA, USA (1997)
7. Altman, I.: The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding. Brooks/Cole, Monterey, California (1975)
8. Altman, I.: Privacy Regulation: Culturally Universal or Culturally Specific? Journal of Social Issues **3**(3), 66–84 (1977)
9. Appelt, W.: WWW Based Collaboration with the BSCW System. In: SOFSEM '99: Proceedings of the 26th Conference on Current Trends in Theory and Practice of Informatics on Theory and Practice of Informatics, pp. 66–78. Springer-Verlag, London, UK (1999)
10. Begole, J.B., Tang, J.C., Smith, R.B., Yankelovich, N.: Work Rhythms: Analyzing Visualizations of Awareness Histories of Distributed Groups. In: CSCW '02: Proceedings of the 2002 ACM Conference on Computer Supported Cooperative Work, pp. 334–343. ACM, New York, NY, USA (2002). DOI http://doi.acm.org/10.1145/587078.587125
11. Bellman, S., Johnson, E., Kobrin, S., Lohse, G.: International Differences in Information Privacy Concerns: A Global Survey of Consumers. The Information Society **20**(5), 313–324 (2004)
12. Bellotti, V.: What You Don't Know Can Hurt You: Privacy in Collaborative Computing. In: HCI '96: Proceedings of HCI on People and Computers XI, pp. 241–261. Springer-Verlag, London, UK (1996)
13. Bellotti, V.: Design for Privacy in Multimedia Computing and Communications Environments. In: P.E. Agre, M. Rotenberg (eds.) Technology and Privacy: The New Landscape, pp. 63–98. MIT Press, Cambridge, MA, USA (1997)
14. Bellotti, V., Sellen, A.: Design for Privacy in Ubiquitous Computing Environments. In: ECSCW '93: Proceedings of the Third European Conference on Computer-Supported Cooperative Work, pp. 77–92. Kluwer Academic Publishers, Norwell, MA, USA (1993)
15. Boyle, M., Edwards, C., Greenberg, S.: The Effects of Filtered Video on Awareness and Privacy. In: CSCW '00: Proceedings of the 2000 ACM Conference on Computer Supported Cooperative Work, pp. 1–10. ACM, New York, NY, USA (2000). DOI http://doi.acm.org/10.1145/358916.358935
16. Boyle, M., Greenberg, S.: The Language of Privacy: Learning from Video Media Space Analysis and Design. ACM Trans. Computer-Human Interaction **12**(2), 328–370 (2005). DOI http://doi.acm.org/10.1145/1067860.1067868
17. Cadiz, J.J., Gupta, A., Grudin, J.: Using Web Annotations for Asynchronous Collaboration Around Documents. In: CSCW '00: Proceedings of the 2000 ACM Conference on Computer Supported Cooperative Work, pp. 309–318. ACM, New York, NY, USA (2000). DOI http://doi.acm.org/10.1145/358916.359002
18. Calore, M.: Privacy Fears Shock Facebook. Wired News (2006). http://www.wired.com/science/discoveries/news/2006/09/71739
19. Consolvo, S., Smith, I.E., Matthews, T., LaMarca, A., Tabert, J., Powledge, P.: 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, pp. 81–90. ACM, New York, NY, USA (2005). DOI http://doi.acm.org/10.1145/1054972.1054985
20. Cranor, L.F., Reagle, J., Ackerman, M.S.: Beyond Concern: Understanding Net Users' Attitudes About Online Privacy. AT&T Labs-Research Technical Report **TR 99.4.1** (1999)
21. Danis, C.M.: Extending the Concept of Awareness to Include Static and Dynamic Person Information. SIGGROUP Bulletin **21**(3), 59–62 (2000). DOI http://doi.acm.org/10.1145/605647.605657
22. Diffie, W., Hellman, M.E.: Privacy and Authentication: An Introduction to Cryptography. Proceedings of the IEEE **67**(3), 397–427 (March 1979)
23. Dix, A.J.: Information Processing, Context And Privacy. In: INTERACT '90: Proceedings of the IFIP TC13 Third International Conference on Human-Computer Interaction, pp. 15–20. North-Holland Publishing Co., Amsterdam, The Netherlands (1990)

24. Dourish, P.: Culture And Control In A Media Space. In: ECSCW ‘93: Proceedings of the Third European Conference on Computer-Supported Cooperative Work, pp. 125–137. Kluwer Academic Publishers, Norwell, MA, USA (1993)
25. Dourish, P., Anderson, K.: Privacy, Security... and Risk and Danger and Secrecy and Trust and Identity and Morality and Power: Understanding Collective Information Practices. Institute for Software Research (ISR) Technical Report, University of California, Irvine **UCI-ISR-05-1** (2005)
26. Dourish, P., Bly, S.: Portholes: Supporting Awareness in a Distributed Work Group. In: CHI ‘92: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 541–547. ACM, New York, NY, USA (1992). DOI http://doi.acm.org/10.1145/142750.142982
27. Edwards, W.K.: Policies and Roles in Collaborative Applications. In: CSCW ‘96: Proceedings of the 1996 ACM Conference on Computer Supported Cooperative Work, pp. 11–20. ACM, New York, NY, USA (1996). DOI http://doi.acm.org/10.1145/240080.240175
28. Eggen, B., van Mensvoort, K.: Making Sense of What is Going Around. In: P. Markopoulos, B. de Ruyter, W. Mackay (eds.) Awareness Systems: Advances in Theory, Methodology and Design. Springer-Verlag (2008)
29. Fisher, D., Dourish, P.: Social and Temporal Structures in Everyday Collaboration. In: CHI ‘04: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 551–558. ACM, New York, NY, USA (2004). DOI http://doi.acm.org/10.1145/985692.985762
30. Fox, S.: Trust and Privacy Online: Why Americans Want to Rewrite the Rules. Pew Internet & American Life Project (2000)
31. Froehlich, J., Dourish, P.: Unifying Artifacts and Activities in a Visual Tool for Distributed Software Development Teams. In: ICSE ‘04: Proceedings of the 26th International Conference on Software Engineering, pp. 387–396. IEEE Computer Society, Washington, DC, USA (2004)
32. Gaver, W., Moran, T., MacLean, A., Lövstrand, L., Dourish, P., Carter, K., Buxton, W.: Realizing a Video Environment: EuroPARC’s RAVE System. In: CHI ‘92: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 27–35. ACM, New York, NY, USA (1992). DOI http://doi.acm.org/10.1145/142750.142754
33. Goffman, E.: The Presentation of Self in Everyday Life. Doubleday, Garden City, New York (1959)
34. Grinter, R.E., Palen, L.: Instant Messaging In Teen Life. In: CSCW ‘02: Proceedings of the 2002 ACM Conference on Computer Supported Cooperative Work, pp. 21–30. ACM, New York, NY, USA (2002). DOI http://doi.acm.org/10.1145/587078.587082
35. Gross, T., Wirsam, W., Graether, W.: AwarenessMaps: Visualizing Awareness In Shared Workspaces. In: CHI ‘03: CHI ’03 Extended Abstracts on Human Factors in Computing Systems, pp. 784–785. ACM, New York, NY, USA (2003). DOI http://doi.acm.org/10.1145/765891.765990
36. Heath, C., Luff, P.: Disembodied Conduct: Communication Through Video in a Multi-Media Office Environment. In: CHI ‘91: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 99–103. ACM, New York, NY, USA (1991). DOI http://doi.acm.org/10.1145/108844.108859
37. Herbsleb, J.D., Atkins, D.L., Boyer, D.G., Handel, M., Finholt, T.A.: Introducing Instant Messaging And Chat In The Workplace. In: CHI ‘02: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 171–178. ACM, New York, NY, USA (2002). DOI http://doi.acm.org/10.1145/503376.503408
38. Hong, J.I., Ng, J.D., Lederer, S., Landay, J.A.: Privacy Risk Models for Designing Privacy-Sensitive Ubiquitous Computing Systems. In: DIS ‘04: Proceedings of the 2004 Conference on Designing Interactive Systems, pp. 91–100. ACM Press, New York, NY, USA (2004). DOI http://doi.acm.org/10.1145/1013115.1013129
39. Hudson, S.E., Smith, I.: 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, pp. 248–257. ACM, New York, NY, USA (1996). DOI http://doi.acm.org/10.1145/240080.240295

40. Iachello, G., Abowd, G.D.: 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, pp. 91–100. ACM Press, New York, NY, USA (2005). DOI http://doi.acm.org/10.1145/1054972.1054986
41. Johnson, D.G.: Computers and Privacy. In: Computer Ethics. Prentice-Hall, Englewood Cliffs, NJ (1985)
42. Kahn, J.: Yahoo helped Chinese to Prosecute Journalist. International Herald Tribune (2005)
43. Kobsa, A., Teltzrow, M.: Contextualized Communication of Privacy Practices and Personalization Benefits: Impacts on Users' Data Sharing and Purchase Behavior. In: D. Martin, A. Serjantov (eds.) Privacy Enhancing Technologies: Fourth International Workshop, PET 2004, LNCS 3424, pp. 329–343. Springer (2005). DOI http://dx.doi.org/10.1007/11423409_21
44. Langheinrich, M.: Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems. In: UbiComp '01: Proceedings of the 3rd International Conference on Ubiquitous Computing, pp. 273–291. Springer-Verlag, London, UK (2001)
45. Lau, T., Etzioni, O., Weld, D.S.: Privacy Interfaces For Information Management. Communications of the ACM **42**(10), 88–94 (1999). DOI http://doi.acm.org/10.1145/317665.317680
46. Lederer, S., Hong, J., Dey, A.K., Landay, J.: Personal Privacy through Understanding and Action: Five Pitfalls for Designers. Personal Ubiquitous Computing **8**(6), 440–454 (2004). DOI http://dx.doi.org/10.1007/s00779-004-0304-9
47. Lederer, S., Mankoff, J., Dey, A.K.: Towards a Deconstruction of the Privacy Space. In: Ubicomp 2003 Workshop on Ubicomp Communities: Privacy as Boundary Negotiation (2003)
48. Lederer, S., Mankoff, J., Dey, A.K.: 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, pp. 724–725. ACM, New York, NY, USA (2003). DOI http://doi.acm.org/10.1145/765891.765952
49. Lederer, S., Mankoff, J., Dey, A.K., Beckmann, C.: Managing Personal Information Disclosure In Ubiquitous Computing Environments. Technical Report, Computer Science Division, University of California, Berkeley **UCB-CSD-03-1257** (2003)
50. Lee, A., Girgensohn, A., Schlueter, K.: NYNEX Portholes: Initial User Reactions and Redesign Implications. In: GROUP '97: Proceedings of the International ACM SIGGROUP Conference On Supporting Group Work, pp. 385–394. ACM, New York, NY, USA (1997). DOI http://doi.acm.org/10.1145/266838.267359
51. Lessig, L.: Code and Other Laws of Cyberspace. Basic Books, Inc., New York, NY, USA (1999)
52. Mantei, M.M., Baecker, R.M., Sellen, A.J., Buxton, W.A.S., Milligan, T., Wellman, B.: Experiences in the Use of a Media Space. In: CHI '91: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 203–208. ACM, New York, NY, USA (1991). DOI http://doi.acm.org/10.1145/108844.108888
53. Mason, R.O.: Four Ethical Issues of the Information Age. MIS Quarterly **10**(1), 5–12 (1986)
54. Metaxas, G., Markopoulos, P.: Abstractions of Awareness. In: P. Markopoulos, B. de Ruyter, W. Mackay (eds.) Awareness Systems: Advances in Theory, Methodology and Design. Springer-Verlag (2008)
55. Milberg, S.J., Burke, S.J., Smith, H.J., Kallman, E.A.: Values, Personal Information Privacy, and Regulatory Approaches. Communications of the ACM **38**(12), 65–74 (1995). DOI http://doi.acm.org/10.1145/219663.219683
56. Nardi, B.A., Whittaker, S., Bradner, E.: Interaction and Outeraction: Instant Messaging in Action. In: CSCW '00: Proceedings of the 2000 ACM Conference on Computer Supported Cooperative Work, pp. 79–88. ACM, New York, NY, USA (2000). DOI http://doi.acm.org/10.1145/358916.358975
57. Neale, D.C., Carroll, J.M., Rosson, M.B.: Evaluating Computer-Supported Cooperative Work: Models and Frameworks. In: CSCW '04: Proceedings of the 2004 ACM Conference on Computer Supported Cooperative Work, pp. 112–121. ACM, New York, NY, USA (2004). DOI http://doi.acm.org/10.1145/1031607.1031626
58. Negley, G.: Philosophical Views on the Value of Privacy. Law and Contemporary Problems **31**(2), 319–325 (1966)

59. Olson, G.M., Olson, J.S.: Distance Matters. Human-Computer Interaction **15**(2/3), 139–178 (2000)
60. Olson, J.S., Grudin, J., Horvitz, E.: A Study of Preferences for Sharing and Privacy. In: CHI '05: CHI '05 Extended Abstracts on Human Factors in Computing Systems, pp. 1985–1988. ACM, New York, NY, USA (2005). DOI http://doi.acm.org/10.1145/1056808.1057073
61. Olson, J.S., Teasley, S.: Groupware in the Wild: Lessons Learned from a Year of Virtual Collocation. In: CSCW '96: Proceedings of the 1996 ACM Conference on Computer Supported Cooperative Work, pp. 419–427. ACM, New York, NY, USA (1996). DOI http://doi.acm.org/10.1145/240080.240353
62. Palen, L.: Social, Individual and Technological Issues for Groupware Calendar Systems. In: CHI '99: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 17–24. ACM, New York, NY, USA (1999). DOI http://doi.acm.org/10.1145/302979.302982
63. Palen, L., Dourish, P.: Unpacking "Privacy" for a Networked World. In: CHI '03: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 129–136. ACM, New York, NY, USA (2003). DOI http://doi.acm.org/10.1145/642611.642635
64. Patil, S., Kobsa, A.: Instant Messaging and Privacy. In: Proceedings of HCI 2004, pp. 85–88 (2004). http://www.ics.uci.edu/ kobsa/papers/2004-HCI-kobsa.pdf
65. Patil, S., Kobsa, A.: Privacy in Collaboration: Managing Impression. In: The First International Conference on Online Communities and Social Computing (2005)
66. Patil, S., Kobsa, A.: Uncovering Privacy Attitudes and Practices in Instant Messaging. In: GROUP '05: Proceedings of the 2005 International ACM SIGGROUP Conference On Supporting Group Work, pp. 109–112. ACM, New York, NY, USA (2005). DOI http://doi.acm.org/10.1145/1099203.1099220
67. Patil, S., Lai, J.: Who Gets to Know What When: Configuring Privacy Permissions in an Awareness Application. In: CHI '05: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 101–110. ACM, New York, NY, USA (2005). DOI http://doi.acm.org/10.1145/1054972.1054987
68. Pinelle, D., Gutwin, C.: Designing for Loose Coupling in Mobile Groups. In: GROUP '03: Proceedings of the 2003 International ACM SIGGROUP Conference On Supporting Group Work, pp. 75–84. ACM, New York, NY, USA (2003). DOI http://doi.acm.org/10.1145/958160.958173
69. Rachels, J.: Why Privacy Is Important. Philosophy and Public Affairs **4**(4), 323–333 (1975)
70. Rittenbruch, M., McEwan, G.: An Historical Reflection of Awareness in Collaboration. In: P. Markopoulos, B. de Ruyter, W. Mackay (eds.) Awareness Systems: Advances in Theory, Methodology and Design. Springer-Verlag (2008)
71. Romero, N., Markopoulos, P.: Grounding Privacy with Awareness. In: P. Markopoulos, B. de Ruyter, W. Mackay (eds.) Awareness Systems: Advances in Theory, Methodology and Design. Springer-Verlag (2008)
72. Samarajiva, R.: Interactivity as though Privacy Mattered. In: P.E. Agre, M. Rotenberg (eds.) Technology and Privacy: The New Landscape, pp. 277–309. MIT Press, Cambridge, MA, USA (1997)
73. Schwartz, B.: The Social Psychology of Privacy. The American Journal of Sociology **73**(6), 741–752 (1968). URL `http://www.jstor.org/stable/2775779`
74. Stone, E.F., Gueutal, H.G., Gardner, D.G., McClure, S.: A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes Across Several Types of Organizations. Journal of Applied Psychology **68**(3), 459–468 (1983)
75. Suchman, L.A.: Plans and Situated Actions: The Problem of Human-Machine Communication. Cambridge University Press, New York, NY, USA (1987)
76. U.S. Department of Health Education and Welfare: Records, Computers and the Rights of Citizens. Report of the Secretary's Advisory Committee on Automated Personal Data Systems **Publication No. 1700–00116** (1973)
77. Warren, S.D., Brandeis, L.D.: The Right to Privacy. Harvard Law Review **4**(5), 193–220 (1890)

78. Westin, A.F.: Privacy and Freedom. Atheneum, New York (1967)
79. Westin, A.F.: Harris-Equifax Consumer Privacy Survey 1991 (1991)
80. Wickramasuriya, J., Datt, M., Mehrotra, S., Venkatasubramanian, N.: Privacy Protecting Data Collection in Media Spaces. In: MULTIMEDIA ‘04: Proceedings of the 12th Annual ACM International Conference On Multimedia, pp. 48–55. ACM, New York, NY, USA (2004). DOI http://doi.acm.org/10.1145/1027527.1027537