Interacting with Computers 22(3), 206-217

Enhancing Privacy Management Support in Instant Messaging

Sameer Patil, Alfred Kobsa

Department of Informatics, University of California, Irvine CA 92697 USA

Abstract

Instant Messaging (IM) is a useful tool for collaborative work. However, the awareness and communication features of IM pose a tension with privacy desires. Inadequate support for managing privacy could lead to suboptimal use of IM and thereby undermine its benefits. We conducted interviews and an Internet survey to understand privacy attitudes and practices in IM usage. Based on the findings from these studies, we designed an IM plugin to improve the support for privacy management in current IM systems. The plugin detects conflicts in privacy preferences, notifies the parties involved, and allows negotiation of a resolution. It also encrypts the communication channels and archives, allows different privacy preferences for different contact groups, and provides visualizations to facilitate the comparison of one's own IM activities with those of any IM contact group. A usability evaluation of the plugin indicated that it succeeds in its goal of providing IM users with better privacy management.

Key words: privacy, instant messaging, IM, privacy management, impression management, computer-supported communication, computer supported collaborative work, CSCW

1 Introduction

Instant Messaging (IM) was popularized by adolescents but today it is used by people of all ages. While its initial focus was on supporting social ties among friends, it is increasingly being adopted as a tool for collaborative work due the utility of its awareness and communication mechanisms (Herbsleb et al.,

Email addresses: patil@uci.edu (Sameer Patil), kobsa@uci.edu (Alfred Kobsa).

2002). Consequently, IM use is no longer limited to the home but has expanded to include workplaces and educational institutions.

The lightweight awareness and communication mechanisms of IM offer a host of benefits for improving the effectiveness of collaborative work. IM allows one to gauge the availability of colleagues and adjust communication with them accordingly. This facilitates faster turnaround for quick, short queries. IM can also facilitate increased informal interaction among co-workers, both local and remote. Increased informal communication is known to have a positive impact on collaboration (Kraut et al., 1988). Unlike face-to-face meetings or telephone conversations, IM makes it easier to multi-task by maintaining multiple simultaneous conversations. Further, IM can reduce the costs of long-distance communication and of travel to locations of remote collaborators.

With the growing recognition of IM's potential to support collaboration, Enterprise IM systems designed for the organizational setting are becoming a part of corporate intranets. IM is also being embedded into other applications such as web pages (e.g., Hubz http://www.hubz.com), email (e.g., Google Talk® within GMail® http://www.gmail.com), and software development environments (e.g., Jazz (Cheng et al., 2003)). Moreover, IM clients are being run on cell phones and Personal Digital Assistants (PDAs) (Isaacs et al., 2002) allowing one to stay connected with one's IM contacts even when away from a traditional computer.

Both the awareness and the communication features of IM are in tension with people's desire for privacy. For instance, IM increases the awareness that others have regarding one's presence and activities. This may lead to more interruptions and distractions due to inopportune incoming messages or, more severely, to online surveillance. Similarly, one's IM communication could be shared with a third party without one's permission or even knowledge. If not addressed effectively, such privacy concerns can become a barrier to the adoption and use of a system. Focusing on awareness, and paying insufficient attention to privacy aspects of the system, may evoke strong user backlash. A recent example involving the popular social networking site Facebook (http://www.facebook.com) is an excellent case in point. Facebook introduced an awareness feature that automatically presented to each user an aggregation of every single activity of their friends. Tens of thousands of users were outraged and launched a revolt, ranging from online petitions and protest groups to threats of a boycott (Calore, 2006). Facebook eventually backed down and provided users with controls to specify which activities would be shared with whom.

The goal of our work is to analyze privacy attitudes and practices of IM users and enhance the "privacy friendliness" of IM in order to boost its utility, particularly for collaborative work. To achieve this objective, we investigated the nature of privacy concerns among IM users along with the various factors that influence these concerns and used the insights from these studies to design various enhancements to IM privacy management. This paper describes a fully functioning prototype that implements these designs. We also describe the results of a user study conducted to evaluate the usability as well as the anticipated utility of the different privacy-enhancing features that the prototype provides.

2 Related Work

Prior work that is relevant for our purposes can be broken down into three broad themes: studies that report on user experiences with specific awareness systems, theoretical analyses of privacy along with principles and guidelines for system design, and concrete techniques and approaches for system implementation. Each of these themes will be discussed in the following subsections.

2.1 User Studies of Awareness Systems

Initial findings related to privacy were primarily noted as side observations in studies aimed at evaluating experiences with the awareness aspects of systems. Dourish (1993) characterizes privacy controls along a social-technical continuum. On the social side, social pressures and norms are relied upon to prevent misuse of the system. On the technical side, technology prevents attempted misuse. Social controls are likely to work well only within a small, relatively tight-knit community (Ackerman et al., 1997; Dourish, 1993). Even then, they may result in very strong protection behavior such as turning the system off, or altering one's work habits (Mantei et al., 1991). In contrast, technical privacy protections cause increased acceptance and adoption of a system because users have greater trust that the system will protect their privacy (Dourish, 1993). Later studies confirmed that trust in a system is an important implicit factor in privacy assessments (Adams, 1999; Adams and Sasse, 1999; Patil and Lai, 2005).

Palen (1999) 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[1] , partly via practices such as cryptic entries, omissions, defensive scheduling, and partly

[1] Palen (1999) noticed that individuals with unusually restrictive, or liberal, calendar access settings often had immediate colleagues with similar access configurations.

via social anonymity within the organizational context. The system we describe in the paper follows such a socio-technical approach, relying on both social and technical control and enforcement.

Later studies of awareness systems began to target privacy as the primary object of investigation (Adams, 1999; Adams and Sasse, 1999; Consolvo et al., 2005; Lederer et al., 2004; Olson and Teasley, 1996). These studies identified that the relationship with the information recipient, the purpose or usage of information, the context, and the sensitivity of content are important factors in making privacy judgments [2] . In studies specific to IM, Herbsleb et al. (2002) found that the lack of lightweight mechanisms to address privacy is a barrier for setup and adoption. Grinter and Palen (2002) 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. Nardi et al. (2000) found that plausible deniability of presence is used for managing privacy in instant messaging.

2.2 Theory, Principles and Guidelines

Privacy is recognized to be a nuanced and situated concept without a universal definition. The rich body of literature on privacy in the social sciences is testimony to its intricate connections with the broader social context (Dourish and Anderson, 2005). Due to this complexity, technology designers have found it difficult to analyze and frame the privacy issues unveiled by user studies. Researchers have tried to address this problem by attempting to articulate theoretical insights regarding privacy in forms that are more accessible to system designers. For instance, Boyle and Greenberg (2000) describe a vocabulary of privacy that designers can employ for an unambiguous discussion of privacy issues. To suggest ways of thinking about privacy in socio-technical environments, Palen and Dourish (2003) outline a model of privacy that is based on the theory of social psychologist Irwin Altman. It views 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 also compiled various privacy-related findings from user studies into design principles and guidelines in order to allow for better privacy management. Bellotti and Sellen (1993) propose a design framework based on feedback and control regarding information capture, construction, accessibility, and purpose. The purpose of feedback mechanisms is to provide users with information that helps them make judgments regarding privacy, while the purpose of control is to empower them to take appropriate actions to

[2] We found these to apply for IM as well; see Section 3.1.

manage privacy. Langheinrich (2001) draws upon fair information practices (Landesberg et al., 1998) and proposes that privacy-sensitive systems ought to notify their users appropriately, seek user consent, provide choice, allow for user anonymity or pseudonymity, limit scope with proximity and locality, ensure adequate security, and implement appropriate information access. Iachello and Abowd (2005) provide an additional 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. (2004) 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. (2004) describe privacy risk models to analyze how well a system meets such principles or avoids pitfalls. These risk models are a set of questions on information sharing, pertaining to the social and organizational context in which the system is situated, and to the technology which is used to implement the system. To incorporate user perceptions, Adams and Sasse (1999) provide a privacy model based on information sensitivity, information receiver, and information usage, in which each of the three factors interacts with the others. As the following sections will illustrate, our design draws on many of these interrelated principles and guidelines.

2.3 Design Techniques and Approaches

Incorporating 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 and the context.

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

- encryption (e.g., (Borisov et al., 2004));
- access control via preferences, policies, and roles (Edwards, 1996; Wickramasuriya et al., 2004);
- mechanisms to reduce the burden of preference specification such as lightweight interfaces (Lau et al., 1999), or grouping and templates (Olson et al., 2005; Patil and Lai, 2005);
- automatic or manual control of granularity of disclosed information (Consolvo et al., 2005; Dourish, 1993; Lee et al., 1997; Palen, 1999);
- feedback via visualization (Gross et al., 2003), sound (Gaver et al., 1992), intelligent agents (Ackerman and Cranor, 1999), and contextual disclosure

of privacy practices (Kobsa and Teltzrow, 2005);
- distortion of disclosed information (Boyle et al., 2000);
- support for anonymity (or pseudonymity) (Appelt, 1999); and
- modeling-based inference (Begole et al., 2002).

Describing these techniques is beyond the scope of this paper. The reader is referred to the cited works for details. In practice, no single technique can satisfy all requirements and constraints. Our enhancements to IM privacy management combine several of these approaches.

3 Motivation

No prior work has focused exclusively on the study of privacy issues in IM. To fill this knowledge gap, we interviewed and surveyed IM users with the goal of understanding their privacy attitudes, expectations and practices when using IM (Patil and Kobsa, 2004, 2005a,b). Findings from these studies helped us identify privacy concerns and privacy management challenges faced by IM users, and guided us in designing solutions that address these problems. We summarize relevant findings from each study below.

3.1 Interviews

We conducted semi-structured interviews of approximately 90 minutes with seven adults who used IM on a regular basis (Patil and Kobsa, 2004, 2005a). In order to compare and contrast the use of IM in a broad variety of situations, we chose individuals with diverse backgrounds and work environments. Overall, we found that privacy concerns of IM users were influenced by three main factors: who (the person(s) with whom information is exchanged), when and where (the context in which information is exchanged), and what (the content that is communicated).

Subjects' practices revealed a desire to be available in different extents to different groups of people, such as co-workers, family, and friends (Patil and Kobsa, 2004, 2005a). For instance, some of our subjects had reservations about including their superiors in their contact lists. Subjects wished to have control over their availability to others in order to avoid interruption and distraction from the current task. Expectations and practices regarding availability heavily depended on the location, the time, and the (work) context. Moreover, all subjects took into account the sensitivity of the content of their IM conversations. They tried consciously to avoid saying anything over IM that might be potentially harmful in the future. Subjects were aware of, and had accepted, that IM may be monitored by system administrators, or be sniffed off the network. Yet, just as with email, subjects expected that their conversations would only be read by the intended recipient(s). At the same time, they expressed unease at the prospect that these IM conversations could be saved by their contacts. However, they had resigned themselves to the fact that this was something that they could neither know about nor control. All subjects reported switching to a different communication medium for those conversations that they deemed too sensitive for IM.

3.2 Survey

Based on the findings from the interviews, we developed a detailed online questionnaire aimed at capturing a broad sample of adult (18 years and older) IM users (Patil and Kobsa, 2005b). We received 622 valid responses over a period of approximately 3 weeks. Respondents' open-ended justifications for the degree to which they indicated being concerned about privacy revealed the following main factors: sensitivity of content (33%), personal disposition toward privacy (25%), technical understanding (22%), and the potential retention of conversations through archiving or logging (21%). The relative frequencies of each of these four aspects were correlated with respondents' self-rated level of privacy concern ($p < 0.05$).

Respondents' concerns regarding archiving or logging indicate a perceived lack of control over persistence of conversations. In fact, in many cases this led to self-censorship of what was said (echoing our findings from the interviews). For instance, one respondent commented, "*I know that most people do log their IM conversations, so I try and keep that in mind while talking privately with someone about sensitive things.*"

We also found a positive/negative correlation between understanding/misunderstanding of technology, and stated level of privacy concern. Misunderstanding of technology seemed to create a false sense of security leading to lower concern for privacy ($p < 0.001$), whereas correct understanding exposed risks and thus raised privacy concern.

The level of privacy concern also correlated positively with respondents' degree of agreement that their IM behavior is altered by the following factors: workplace policies, the possibility that network traffic may be sniffed, and the ability of others to save their conversations (each $p < 0.01$). As can be expected, an increased concern for privacy is correlated with the proclivity for privacy-enhancing actions and practices. Respondents who were more concerned with privacy were more likely to use encryption, to switch the conversation medium for sensitive conversations, to lock their screens when away from their computer, and to change the default settings of the IM system.

As was the case in the interviews, respondents' expectations regarding privacy differed significantly for different groups of contacts.

3.3 Current Limitations of IM Privacy Management

Findings from our interviews and survey indicate that many IM users have devised practices aimed at alleviating privacy concerns. Some examples include self-censorship, turning IM off, switching the communication medium to avoid a written trail, and maintaining separate IM accounts for different purposes. It could be argued that such practices contribute to suboptimal use of IM. In an organizational context, underuse and circumvention may undermine the gains that the organization expects from its IM deployment. Enhancing privacy management should reduce the need for such tactics. For instance, instead of having to turn IM off to avoid unnecessary interruptions, one should be able to be invisible to most contacts while remaining available to a few critical ones. Instead of switching the communication medium, one should be able to disable archiving during an IM conversation.

Currently, IM systems allow users to manage privacy primarily by specifying "global" preferences for various privacy-affecting factors, such as who is authorized to view information about them, and who is authorized to communicate with them. This approach is not adequate for finer-grained information disclosure preferences and practices, based upon who wants to know what, when, and why (Lederer et al., 2003a). For instance, a single set of privacy preferences does not allow users to express differences in attitudes and behaviors with respect to different groups of IM contacts.

IM users in our study also expressed frustration at the inability to know about, or have control over, the actions of others that are likely to be of concern to them (Consolvo et al., 2005; Patil and Kobsa, 2004, 2005a,b). This frustration revealed other limitations of privacy management in current IM systems. These are the lack of visibility of, and control over, privacy-affecting actions of others and of the ability to adjust preferences seamlessly during ongoing conversations. Thus, IM systems fall into the pitfalls of obscurity and inadequate control pointed out by Lederer et al. (2004). Additionally, the effect of technological understanding that we discovered suggests that making the IM system more transparent to users could facilitate better privacy decisions. Our work is aimed at overcoming these shortcomings.

Another deficiency in current IM systems was uncovered through the survey responses on desired enhancements to IM capabilities. Many respondents indicated that they would like to know when others saved their conversations,

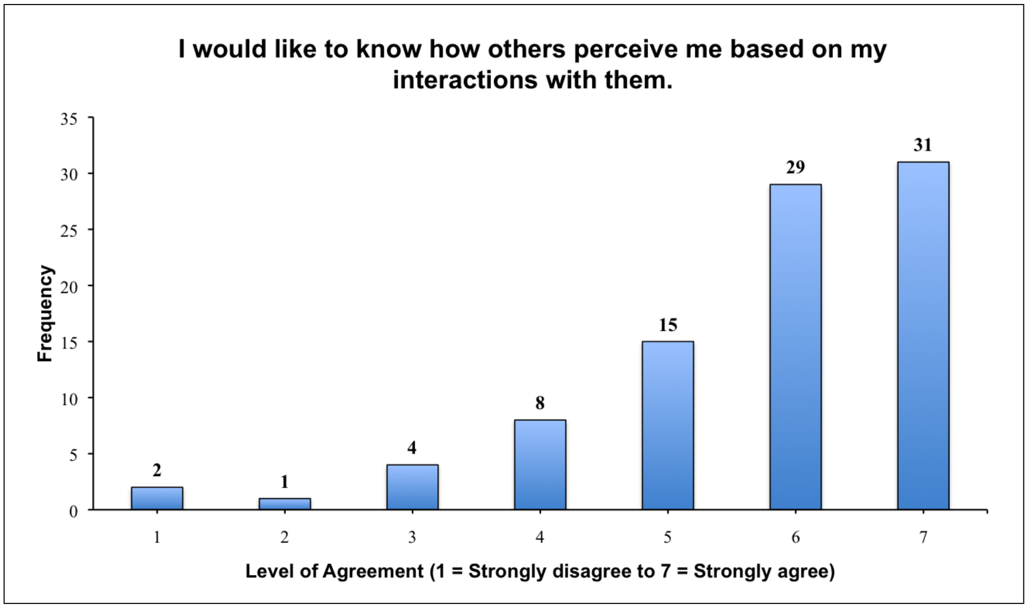


Fig. 1. Level of desire to view how others perceive oneself

to set expiration dates for saved conversations, to compare themselves with their contacts, and to know how they appear to their contacts via IM. As will be discussed below, the notice and negotiation mechanisms that we developed provide support for the two former features while the visualization mechanisms facilitate the latter two aspects.

3.4 Field Study

After the interviews and the online questionnaire, we sought additional validation from a broader industry field study of a collaborative project at a multinational corporation. We looked at around 125 collaborators spread across four sites in the U.S. and one in India. In a survey conducted as part of this research, we found overwhelming support from users for mechanisms that would allow them to judge how they are perceived by others (see Figure 1).

The same survey also indicated that users were not averse to configuring systems by specifying preferences, if this allowed them improved privacy management (see Figure 2). In fact, we found that those who desired tools for better privacy management were more willing to incur the burden of customizing the system (R = 0.58, p < 0.01). These findings provided further support for our design ideas and motivated their implementation into a prototype.

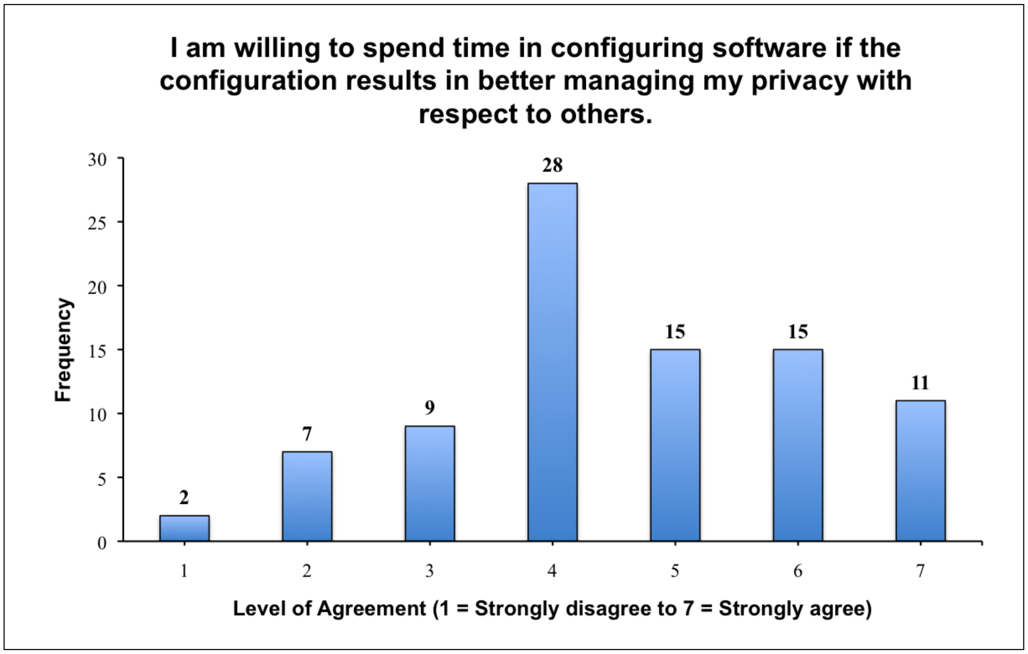


Fig. 2. Willingness to spend time and effort in configuring preferences

4 PRISM

In this section, we present our PRIvacy-Sensitive Messaging system PRISM, which was designed to enhance the support for privacy management for IM users by leveraging the empirical findings described above.

4.1 Overview

Our studies of IM users indicated that several aspects of IM are pertinent to privacy management. These include archiving of conversations, visibility of the actions of others and oneself, and differing attitudes toward different groups of contacts (see Section 3.1). We designed solutions that address each of these aspects with the goal of enhancing support for managing privacy in IM.

In generating our designs, we used the following principles derived from prior research on privacy (Bellotti and Sellen, 1993; Hong et al., 2004; Langheinrich, 2001; Lederer et al., 2004), and from Fair Information Practices (Landesberg et al., 1998):

- *Choice*: Users should be empowered to control aspects of IM that affect their privacy.
- *Notice*: Users should be notified of preferences and actions of others if these affect their privacy.

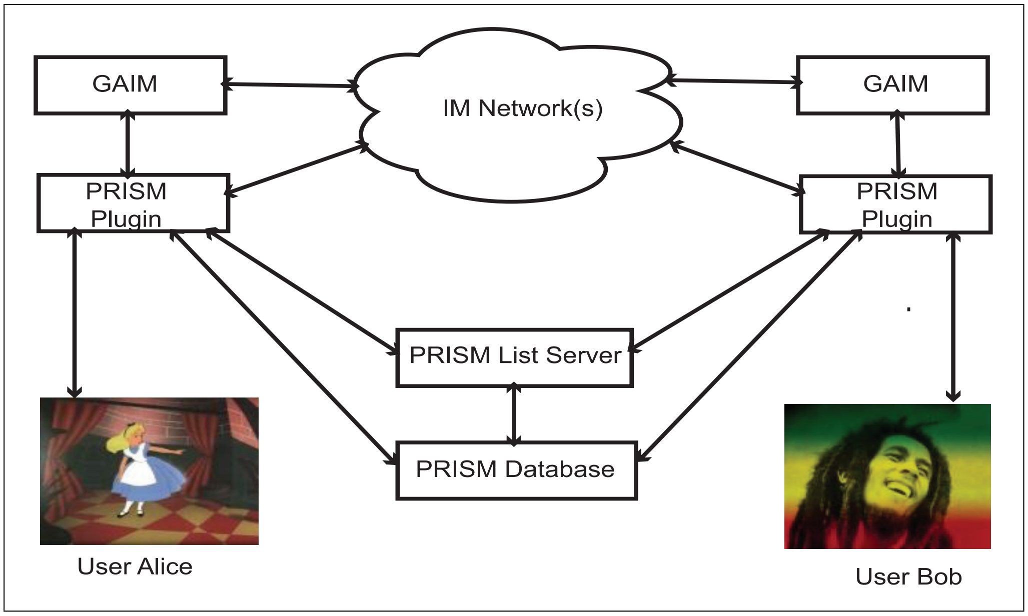


Fig. 3. System architecture of PRISM

- *Negotiation*: When preferences of users conflict with preferences or actions of other users, it should be possible to negotiate solutions to resolve the conflict(s).
- *Revocability*: Users should be able to specify, modify, and/or (re)negotiate privacy-related preferences at any time with minimal effort.

To demonstrate the practical feasibility of our design ideas, we decided to incorporate them into the open-source IM client GAIM (http://gaim.sourceforge.net/), now known as Pidgin (http://www.pidgin.im). We chose GAIM because of its support for plugins, its cross-platform availability, and its ability to access most popular IM networks such as MSN, Yahoo!, AOL, and ICQ. In the following subsections, we first describe the architecture PRISM, and then present the specifics of our design in terms of the functionalities provided.

4.2 System Description

PRISM's extensions to the standard GAIM functionality are packaged as a plugin. The architecture of the system is shown in Figure 3. All events that occur in GAIM are passed through this plugin before being presented to the user. Events that are not trapped are passed through without change (e.g., incoming IM messages are simply displayed to the user). PRISM also uses the IM network to communicate with the PRISM instances of the user's current IM partners. Each such PRISM-specific message is marked with a special prefix. It is relayed as an IM message via GAIM through the IM network and is trapped and processed by the instance of the plugin on the other side. Obviously, such communication will work only if both the sender and the recipient(s) have the plugin installed. Otherwise, those who lack the plugin would see PRISM messages as a regular IM message. To ensure that these messages are sent to PRISM-enabled users only, we currently maintain a server with which each instance of the plugin registers upon launch. Additionally, all running instances of the plugin, as well as the PRISM server, communicate with a database that logs various user actions of interest (e.g., sign-in/sign-off times, times of status changes along with the new status message, etc.). Various visualizations of the activities of a group can be generated from this data (see Section 4.3.6).

It should be noted that as soon as the functionalities that the plugin provides become part of an IM system and protocol, then both the PRISM server and the database will no longer be necessary.

4.3 Functionalities

PRISM adds a host of functionalities to the base IM system in order to enhance support for privacy management.

4.3.1 Notice

In our empirical studies, IM users wished to know more about the actions of others that may affect their privacy. To meet this need, PRISM notifies the user of the choices and the actions of others that may compromise his or her privacy. For example, PRISM can detect conflicts between the preferences of conversation partners regarding whether or not to save the current conversation. If one party opts to save the conversation while another party has conversation logging turned off, PRISM notifies the latter party that the conversation is going to be saved by the other party.

4.3.2 Negotiation

Besides notifying users about conflicting preferences, PRISM also addresses their frustration about not having a say in actions of others that might invade their privacy. This concerns is handled by PRISM's conflict notifications which are accompanied by an interface for users to negotiate with each other to resolve the conflict. For instance, users can negotiate whether or not to save a conversation, and for how long (this will be described in more detail in the example scenario in Section 5).

4.3.3 Control over Archiving Conversations

Negotiation mechanisms are supported by associated controls that allow for the enforcement of the negotiated agreements. Once the decision to prevent archiving of the conversation is negotiated, the ability to save conversations, to copy/paste text, and to capture or print screen shots is turned off for all conversation parties. Obviously, one cannot prevent someone from taking photographs of the screen (just as one cannot prevent someone from installing a voice recorder on their phone). However, the goal is to make logging sufficiently cumbersome and unreliable to become impractical (see Section 6.2.1).

Additionally, PRISM allows expiration dates to be associated with conversation logs. Once the negotiated expiration date of a saved conversation is reached, it is automatically deleted from each location where it is stored [3]. Prior to expiration, PRISM also allows the parties to renegotiate the expiration date should this be deemed necessary.

4.3.4 Contact Expiration

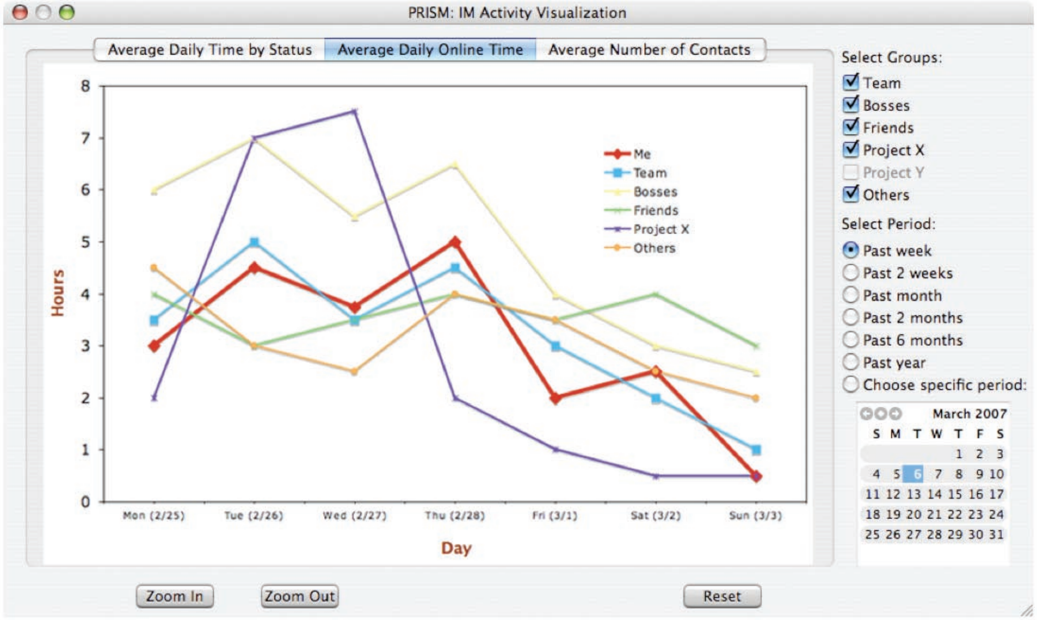
Often, people collaborate with others for a pre-defined length of time. Increased awareness and communication through IM is critical during this period. Thereafter, one may no longer wish to maintain the same heightened level of awareness and communication. Agreeing at the beginning of a collaboration on how long one would be included in someone else's contact list allows one to regain privacy at the end of the collaboration period without incurring the potential social costs of having to block or delete the contact.

PRISM, therefore, allows expiration dates to be associated with contacts as with conversation logs. When the date is reached, the contact will be automatically deleted from the list along with all archived mutual conversations. The expiry period can be negotiated between the parties, and be renegotiated any time prior to expiration.

4.3.5 Encryption

Although encryption of IM messages is gaining support in current IM networks, not all IM systems include it. Even when a system offers encryption, it may be turned off by default. IM programs typically also lack salient indicators that inform the user whether encryption is turned on or off. To overcome these deficiencies, PRISM provides end-to-end encryption for all conversations. This feature addresses the concern, expressed repeatedly in our studies, that a third

[3] A similar BlackBerry®application for cell phone text messaging was launched recently (Business Wire, 2008).



PRISM: IM Activity Visualization

Average Daily Time by Status | Average Daily Online Time | Average Number of Contacts

Select Groups:
☑ Team
☑ Bosses
☑ Friends
☑ Project X
□ Project Y
☑ Others

Select Period:
● Past week
○ Past 2 weeks
○ Past month
○ Past 2 months
○ Past 6 months
○ Past year
○ Choose specific period:

Fig. 4. Visualization of Average Daily Online Time by contact group

party would sniff the conversation off the network. Additionally, for increased system transparency, PRISM displays the familiar lock icon so that users can feel assured of the presence of encryption at a glance.

Most current IM systems store conversation logs in unencrypted text files. This makes it possible for the archived conversation to be read from outside of the IM system (e.g., using a standard text editor). In contrast, PRISM stores conversation logs in encrypted form, ensuring that these can be opened only from within the IM program by providing the appropriate password to unlock the decryption key. This further boosts protection from unauthorized access by third parties.

4.3.6 Visualization of Collective Activities

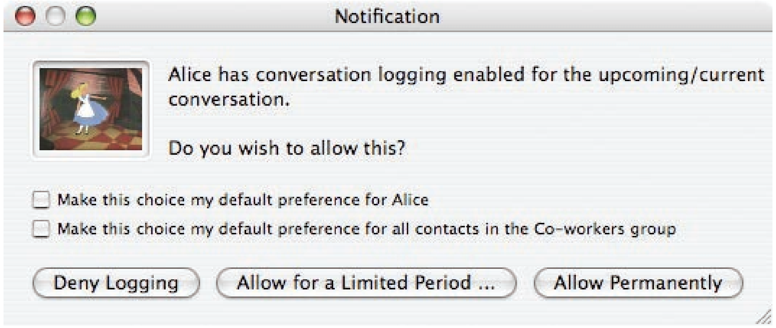
In our surveys and interviews we found that privacy concerns in IM were linked to a desire to manage the impression conveyed by one's IM activities (Kobsa et al., 2010; Patil and Kobsa, 2005a). Impression management includes comparing oneself with others (Leary, 1996). However, the patterns of IM activities, of one's own as well as those of others, are currently not readily visible in IM; all one sees is the current status of one's contacts. This prevents one from gauging the practices of different social groups to which one belongs, and from assessing the kind of impression that is conveyed to those groups based on how one's IM activities compare with the expectations of those groups.

To address this shortcoming, PRISM can generate interactive visualizations of *pooled* IM activities of others. The goal of the visualization feature is to elevate the visibility of the longer-term IM activities of one's social groups and to enable one to view how one's IM activities stand in comparison. Such comparisons could aid in understanding, and tailoring, the impression one conveys. For example, Figure 4 shows the average daily online times for the past week of a user's different contact groups. To facilitate a comparison with different groups, PRISM also displays one's own activities. In Figure 4, the user's own average online time is shown by the red/thick line. It can be seen readily that the user's practices are more or less aligned with his or her team but differ greatly from those of the Project X group, and also to some extent with those of his or her bosses.

The importance of pooling in preserving individual privacy is noteworthy. It sets PRISM apart from existing systems that visualize *individual* IM activities for informational and/or predictive purposes (Begole et al., 2002). In PRISM, it is not possible to drill down to the actions of any particular individual. Thus, pooling preserves the utility of the information regarding IM activities of users without invoking fears of monitoring and surveillance. To further ensure that individual activities cannot be inferred from small groups, PRISM does not display visualizations of activities for groups with fewer than four people. In Figure 4, the user is unable to visualize the activities of the Project Y group for this reason.

The visualization features of PRISM aid privacy management in two ways. Firstly, they elevate the visibility of the actions of others (and oneself) by making it possible to detect longer-term trends and patterns. Non-visual techniques for this purpose would be quite burdensome. As we discussed, lack of visibility was one of the factors that influenced privacy concerns of IM users in our study. Secondly, the visualizations allow one's IM activities to be compared with those of various contact groups. This is important because privacy is shaped by collective experiences and expectations (Palen and Dourish, 2003). Indeed, it has been found that people's valuations of privacy of a piece of personal information is based on a comparison of its deviance from the social norms (Huberman et al., 2005). The visualizations provided by PRISM make collective practices readily visible, and thus facilitate comparisons with one's own actions and promote more informed privacy decisions.

There is a myriad of collective IM practices and behaviors that one may wish to visualize. We have so far implemented visualizations of three of these: average daily online time (shown in Figure 4), IM status when online, and average number of IM contacts. We chose these particular activities because our interview subjects indicated that length of time spent signed into IM as well as status messages were often employed in perceptions of availability and productivity. Other possible privacy-relevant visualizations include the average time elapsed until one responds to an initial incoming message (indicating one's responsiveness), and the average number of simultaneous IM conversa-



Alice has conversation logging enabled for the upcoming/current conversation.

Do you wish to allow this?

☐ Make this choice my default preference for Alice

☐ Make this choice my default preference for all contacts in the Co-workers group

Fig. 5. Notification of preference mismatch

tions (indicating one's availability or busyness). The utility of visualizing a particular IM practice is likely dependent on the context of IM usage, and on attitudes and needs of the user population in question.

We designed PRISM in such a way that programmers can add new visualizations with minimal effort. The PRISM database provides an Application Programming Interface (API) for retrieving collective activity information. This information may then be used to generate and add new visualization modules to PRISM's repertoire. Ultimately, we envision the development of a generic framework for collective visualization that allows *end users* to add visualizations for collective practices and behaviors that are of interest to them.

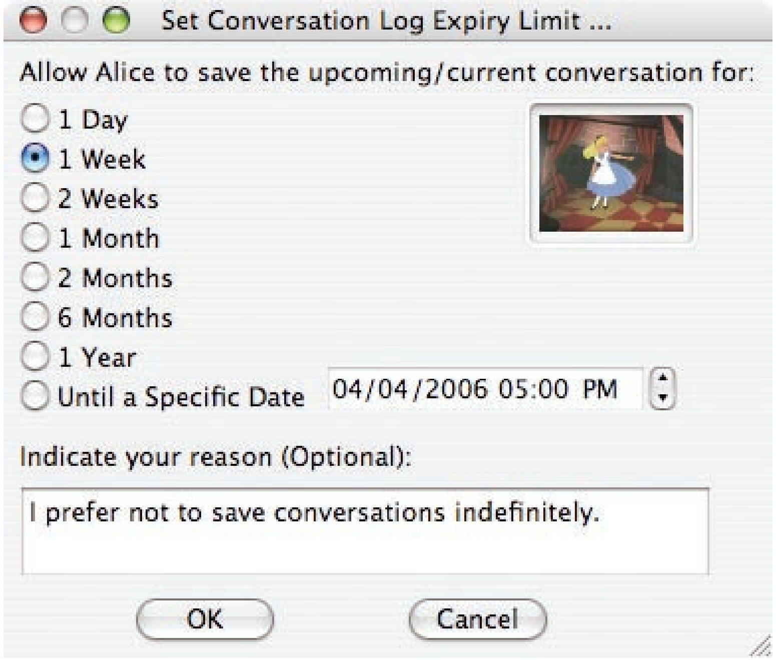
4.3.7 Group-level Preferences

Our empirical studies revealed that people exhibit different privacy desires and practices in relation to different groups of IM contacts. Therefore, PRISM allows users to specify privacy-related preferences at the group level rather than providing only global choices as in most current IM systems. For example, one may elect to be available for colleagues in one's workgroup while being busy for others in the organization.

5 Scenario

To illustrate the manner in which many of the above functionalities manifest themselves at the IM interface, and how they adhere to the principles outlined in Section 4.1, we present an example scenario. Imagine that Alice and Bob are colleagues who collaborate at times, and are on each other's IM contact lists. Both have PRISM installed. Alice prefers to log all her IM conversations automatically, whereas Bob has recently set his preferences not to save any IM conversations (*choice*).

Imagine that Alice wishes to seek clarification from Bob regarding comments



Set Conversation Log Expiry Limit ...

Allow Alice to save the upcoming/current conversation for:

○ 1 Day
● 1 Week
○ 2 Weeks
○ 1 Month
○ 2 Months
○ 6 Months
○ 1 Year
○ Until a Specific Date 04/04/2006 05:00 PM

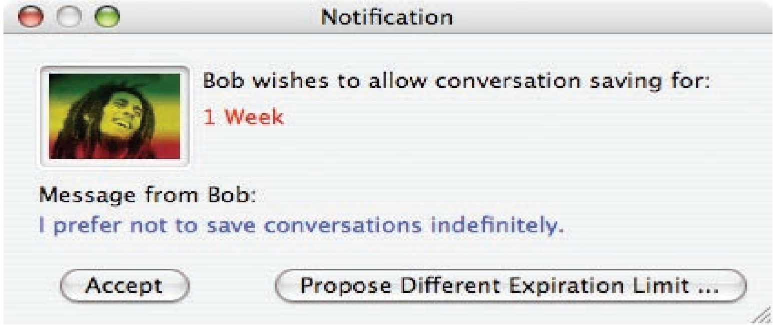
Indicate your reason (Optional):

I prefer not to save conversations indefinitely.

Fig. 6. Setting expiry limit for conversation log

from their boss on a report. She notices in her IM contact list that Bob is online, and opens a conversation window. Before passing on the event to Bob, PRISM notices that there is a mismatch between Alice's and Bob's preferences. Alice prefers to log the conversation automatically, whereas Bob has indicated that he prefers no logging. Thus, before the conversation can be started, PRISM informs Bob that Alice wishes to log the conversation (*notice*), and seeks his permission to do so (*choice*, see Figure 5). At this point, Bob has several options. He can choose to let Alice save this particular conversation. Or, he may decide that he trusts Alice enough so that he can let her save this and all future conversations without being notified of the preference mismatch every time. Alternatively, he can choose to deny Alice the permission to save the conversation. In this case, Alice will be notified that Bob did not wish to have the conversation saved. If Alice chooses to accept Bob's decision, the ability to save the conversation will be disabled for both Bob and Alice.

PRISM further allows Alice and Bob to go beyond a mere yes or no decision. Bob can allow Alice to save the conversation, but only for a specified period, or until a specific date, and optionally specify a reason for his decision (see Figure 6). Alice is informed accordingly (see Figure 7). She can then choose to accept Bob's decision, or to negotiate an alternate date along with an optional reason. The negotiation proceeds back and forth until Alice and Bob reach an agreement regarding whether the conversation can be saved, and, if so, for how long (*negotiation*). To avoid the same negotiation in the future, PRISM allows Alice and Bob to use the result of the negotiation as the default choice


Notification

Bob wishes to allow conversation saving for:
1 Week

Message from Bob:
I prefer not to save conversations indefinitely.

Fig. 7. The choice made by the remote user

in future interactions. This can be done at the individual level, or for the entire group to which Alice or Bob belong in each other's respective contact lists (see Figure 5).

The content of the negotiation itself is not logged. When the mutually accepted expiration date of the conversation is reached, the conversation is automatically deleted. At any point prior to expiration, either Alice or Bob can renegotiate a new expiration date (*revocability*).

Furthermore, PRISM allows Alice and Bob to modify their choices at any point during the conversation, i.e., either of them can decide to revoke their permission to log the conversation (*revocability*). Any dialogue that takes place thereafter will not be saved. For instance, even when Bob initially allows Alice to save the conversation, at a later point in the conversation he may withdraw this permission because he wishes to comment on their boss off the record. Conversely, permission to save could also be requested, and granted, in the middle of a conversation. All future dialogue will then be logged. Thus, after Bob is done commenting about their boss off the record, Alice might request the resumption of conversation saving (*revocability*).

6 Discussion

PRISM adds a new level of privacy protection and structured negotiation to an established informal electronic communication medium. We discuss below the two most salient aspects of PRISM, namely, negotiation and control over archiving.

6.1 Negotiation

The explicit nature of negotiation in PRISM may seem counter to the nuanced and implicit manner in which such negotiations normally take place, e.g., in face-to-face communication. Privacy negotiations that PRISM supports in a structured manner could alternatively also be carried out in plain IM. No extra dialogs would be needed, and negotiations could, in theory, be more nuanced owing to free-text form. However, it is cumbersome to translate the consensus reached in free-form negotiation into a format that the system can understand and enforce (and this would have to be done outside of the IM window). Moreover, negotiating via IM would make it difficult to guarantee privacy safe zone practices (Cranor et al., 2006), such as not allowing the negotiation to be archived (and requests to the system to establish such a zone would again have to be made outside the IM window). It should also be noted that explicit negotiation is already present, and frequently used, in other software systems, such as in Microsoft Outlook® for scheduling meetings. Further, negotiation comes into play in PRISM only in cases where conflicting preferences are detected. The frequency with which negotiations are encountered is further reduced by the fact that the negotiating parties may choose to apply the results of a negotiation to all future conflicts about conversation archiving (see Figure 5).

Predicting one's preferences in advance is difficult. All systems that require users to specify their preferences upfront face this issue. Yet, Lederer et al. (2003b) showed that *a-priori* manual configuration of privacy preferences is better than automatic strategies, especially for information that users deem more important. PRISM attempts to provide additional convenience by making it easier to adjust preferences and to renegotiate past decisions.

Finally, the explicit communication of one's preferences to others (e.g., one's choice to save conversations) could be viewed as undermining one's privacy. However, such notification is provided only to those parties whose privacy could be affected by the choice; PRISM chooses to follow the principle of reciprocity to ensure fairness and equitability.

6.2 Control over archiving

As the continued failure to achieve foolproof Digital Rights Management (DRM) aptly demonstrates, users with sufficient technical skill and perseverance may be able to hack the system and violate privacy agreements negotiated through PRISM. As Loo (2008) summarized, "*technology will never cure all [...] security ills. It will take a coordinated effort involving corporations, manufacturers, employers, and end users to fight the fight.*" PRISM currently uses the two techno-social measures discussed below to minimize the likelihood of circumvention.

6.2.1 Technical measures to increase the burden of circumvention

In general, elevating the cost of circumvention decreases the likelihood that people will attempt it. PRISM significantly raises the time and effort needed for technical circumvention. As mentioned above, the disabling of conversation archiving can be circumvented by taking photos of the conversation on the screen (or merely taking written notes). Doing so is quite burdensome though, and, in contrast with textual archives, such a photo-log is not amenable to easy reading, browsing, searching, quoting etc.

6.2.2 Social and normative controls

The agreements reached through PRISM are not between the system and the user, or between a store and a buyer, but between two *people*. Since these people are in each other's IM contact lists, it is safe to assume a social relationship between them. This implies that an attempt to circumvent an agreement could have social costs if it were discovered, regardless of whether or not the attempt was successful (Dourish, 1993). Additionally, in an institutional context, policies for IM usage could include penalties for attempts to bypass PRISM-negotiated agreements. Finally, telecommunication laws could include punitive measures against bypass attempts and/or deny admissibility in legal proceedings to information obtained by circumventing a negotiated agreement (as is currently the case for phone conversations recorded illegally by law enforcement officials).

7 User Evaluation

We conducted an attitudinal user study to evaluate the extent to which the added enhancements of PRISM can be expected to succeed in their goal of improving privacy management.

7.1 Study Description

Twenty-two individuals (15 males and 7 females) participated in the study. The participants were drawn from a large public university community and comprised of students, faculty, staff, and their friends and relatives. Their ages ranged from 22 to 41 years. Participation was restricted to those 22 years of age or older. The primary rationale behind this restriction was to filter out most of the undergraduate population since prior research suggests that undergraduates have markedly laxer privacy attitudes and behaviors (Patil and Kobsa, 2004, 2005a). Moreover, a main driving force behind PRISM's enhancements is supporting IM usage in collaborative work. The 22-year age limit also substantially increased the likelihood that the participants will have at least some type of working experience despite being from the university community. Since the concept of privacy is known to be culture-dependent, we further restricted participation to those who had lived in the U.S. for five years or longer in order to limit cultural variation. Prior research suggests that five years is a reasonable length of time to assume acclimatization to the host culture (Khan and Khan, 2007).

Each participant was paid $10 in cash. As an incentive to learn about PRISM attentively, participants were also promised a $5 bonus for the three most creative ideas to further improve PRISM, to be selected at the completion of the entire study.

Participants were shown a 15-minute video describing how each feature of PRISM works. To avoid bias, the video did not mention any connection of the features to privacy, nor were the participants informed that the design motivation behind PRISM was to improve privacy management. After watching the video, participants answered five pre-designed questions on PRISM. These questions were meant to test the extent to which they had understood the explanations in the video, and also to spur discussion regarding any aspects that needed to be clarified or explained in more detail. Afterwards, participants were given a chance to ask any other questions (the answers given did not explicitly touch on the connection to privacy). Once all questions had been answered, participants were made to watch the original video a second time to reinforce and refine their understanding.

Thereafter, participants first filled out a questionnaire that sought feedback on PRISM along with a few questions meant to validate the accurate understanding of how PRISM works. Some of the validation questions were drawn from the questions asked in between the two video screenings while the rest were different. Upon completion of the first questionnaire, a second questionnaire was administered to collect demographic information. The second questionnaire also asked about attitudes regarding privacy concerns in e-Commerce using the survey instrument of Smith et al. (1996), and about privacy concerns from different groups of people (e.g., friends, family, superiors etc.). Privacy issues were thus brought to attention in an explicit manner only at the very end of the study, so as not to bias users' attitudes toward PRISM.

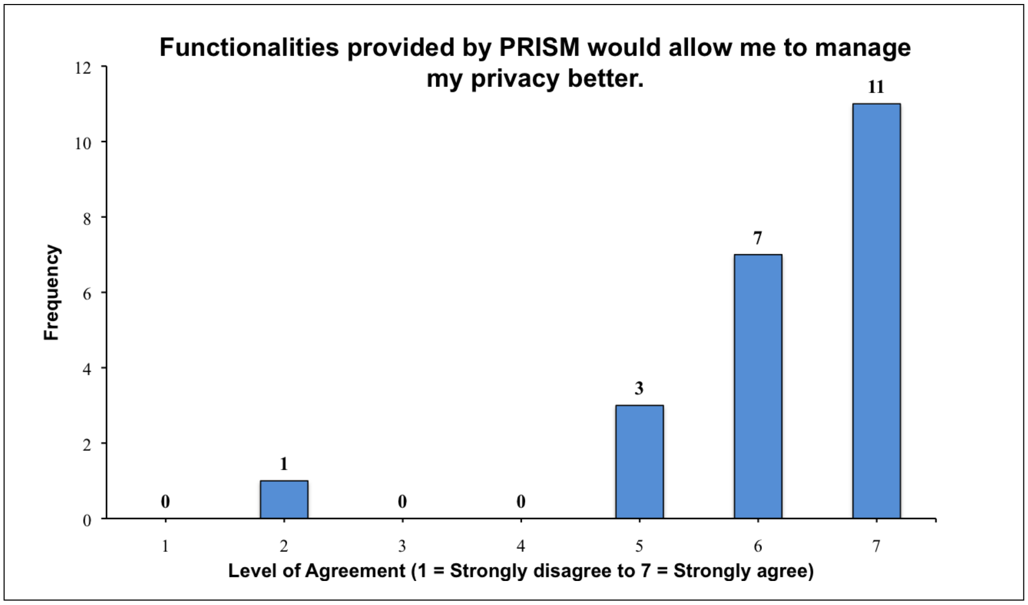


Fig. 8. Users indicate that PRISM improves IM privacy

7.2 Results

The results indicate that users believe that PRISM offers improved IM privacy management. Figure 8 shows that most of our participants strongly agreed that functionalities provided by PRISM allow better privacy management. We also found a statistically significant high correlation between e-Commerce privacy concern, as indicated by the participants' total score on the Smith et al. (1996) scale, and their agreement with the statement "Functionalities provided by PRISM would allow me to manage my privacy better" ($r = 0.52$, $p < 0.014$). The correlation is even stronger for the "Improper Access" subscore of the scale ($r = 0.63$, $p < 0.002$). The former implies that the perceived utility of PRISM increases with "privacy-mindedness" and the latter suggests that PRISM is deemed especially successful in addressing concerns regarding access to information on one's presence, activities and conversations.

We were also heartened to read participant comments regarding PRISM's utility in the work context:

> *"For work I can see the benefit of keeping conversation & having those deleted by a certain date."*

> *"If I was using it a lot and in a work environment with sensitive subject matter, I would use it."*

These comments suggest that the utility of PRISM is likely to be even higher in workplace settings, thus supporting our aim of improving IM as a tool for workplace collaboration.

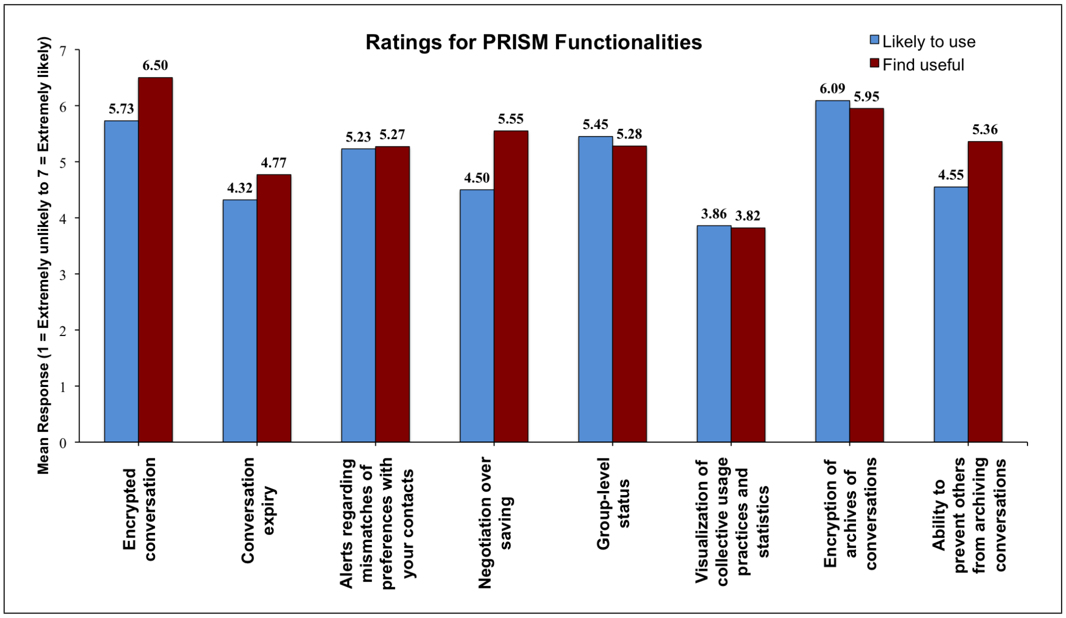


Fig. 9. Utility and Likely Use of PRISM Functionalities

At a finer level, all individual functionalities of PRISM discussed earlier received high scores from participants, both regarding their perceived utility and their likelihood of usage (see Figure 9). The only exception perhaps is the visualization of collective usage practices and statistics, which only received mid-level scores. This may be attributed to users' unfamiliarity with this paradigm and consequential hesitance about its merits. Perhaps the participants could not yet think of suitable IM activities for creating their own visualizations. It is also likely that the learning curve for this feature is rather steep. As users gain more experience with it, we may be able to include popular user-generated visualizations in future versions of PRISM.

We also noted that the utility of features of PRISM that facilitate privacy from unwanted parties (viz., encryption of the conversation channel and conversation archives) showed statistically significant correlations with the "Improper Access" subscore (each $r > 0.58$, $p < 0.01$). Similarly, the utility of features of PRISM that pertain to control over conversation archives (viz., conversation expiry, encrypted archives and preventing others from saving conversations) showed statistically significant correlations with the "Unauthorized Secondary Use" subscore of the Smith et al. (1996) scale (each $r > 0.41$, $p < 0.05$). Both of these subscores also correlate significantly with the utility of the group-level preference specification feature (each $r > 0.41$, $p < 0.05$). This seems to suggest that specifying preferences at the group level may alleviate concerns regarding access to one's presence and online activities as portrayed through IM.

We also found that the perceived utility of PRISM for improving privacy management showed a statistically signification correlation with concerns regarding how others view oneself based on one's IM activities ($r = 0.45$, $p < 0.05$). In addition, the correlation of the perceived utility with the tendency to compare one's IM practices with those of others approaches statistical significance ($r = 0.4$, $p < 0.07$). Yet, the visualization feature that shows how others view oneself and facilitates comparisons received only average scores. As discussed above, we suspect that this is due to the novelty of the feature. We also noted that participants' comments indicate that they found the negotiations a bit cumbersome, which explains the gap between the perceived utility and likelihood of usage of this feature in Figure 9. Therefore, future versions of PRISM ought to work on ways to further reduce the burden of negotiation.

At the interpersonal level, we found that the utility of group-level preference specifications, alerts regarding preference mismatches, and encryption of archives correlated positively with privacy concerns from various categories of contacts such as friends, family, peers, superiors and subordinates ($p < 0.05$). However, there was no correlation in the case of significant others. Moreover, the utility of all features of PRISM, except conversation expiry and visualizations, correlates with privacy concerns from one's ex(es) (p is between 0.01 to 0.1 for the various features). These findings underscore the need to provide a suite of privacy enhancements like in PRISM, in order to cater to the differential utility of each enhancement in supporting privacy needs and expectations for different types of interpersonal relationships.

Finally, we found no notable effects based on age or gender.

8 Conclusion and Outlook

Awareness and communication features of IM are in tension with users' desire for privacy. Previous research of ours had revealed that IM users currently underutilize the full potential of IM in their workplace usage, and resort to escape strategies to maintain privacy. We also found that from a privacy point of view, IM systems need several improvements: specifically, better visibility of actions of others and oneself, and the support for different privacy preferences with respect to different groups of contacts. Current privacy management support in IM systems treats these aspects inadequately. It operates merely through global preference specification and allows little control over, and knowledge of, actions of others that might affect one's privacy. Privacy management in current IM systems also does not seem to be grounded in established privacy-related HCI principles.

In contrast, our IM plugin PRISM empowers IM users to manage privacy more effectively, and more equitably, by adhering to the principles of choice, notice, negotiation and revocability. In particular, it provides increased visibility for privacy-affecting actions of others, the capability to associate expiration dates with conversation logs and with contacts, mechanisms to negotiate conflicting privacy preferences, encrypted communication channels and encrypted logs, increased visibility for one's own actions in relation to those of one's contacts, and the ability to manage privacy differently for different groups of contacts. PRISM is the first attempt at translating findings from user studies on privacy concerns in IM into a comprehensive system. It aims to serve as a stepping-stone that inspires further exploration of the design space to improve privacy management in IM. User attitudes toward PRISM indicate strong support for its utility in enhancing IM privacy management. An actual deployment is needed to further ascertain in-context adoption and usage.

Currently, PRISM only allows a few preferences (namely, status, and conversation logging) to be set differently for different groups of contacts. Our goal is to make all IM preferences available for differential specification by group. In order to reduce the burden of spelling out and managing a large number of different preferences for various groups, we plan to employ a template approach such that settings inherited from a global template can be adjusted appropriately with minimal effort. Finally, we intend to support negotiation between more than two parties. In such cases, we face interesting decisions such as whether to resolve conflicts in multi-party chats democratically (i.e. the majority prevails), or conservatively (i.e., the most privacy sensitive choice prevails).

PRISM provides generic privacy enhancements that do not rely on specifics of any particular IM system. Different IM systems differ in the details of their protocols, and of their server implementations. Thus, it is quite challenging to provide a common cross-IM experience. For example, some IM systems allow broadcasting the length of idle time, but others do not; some IM systems allow multiple simultaneous logins, and others do not. We found that catering to the lowest common denominator limits the extent to which the client side can add, or improve, privacy management features. Shared open and extensible standards for IM implementations may be one solution for addressing this challenge. Alternatively, a custom IM server and protocol that serves as a superset of all protocols may need to be developed. In essence, we advocate that PRISM features be integrated into every IM system. This can only be achieved by tight co-evolution of the IM protocol, the IM server, and the IM client.

9 Acknowledgments

We acknowledge the contribution of all those involved in programming PRISM. We also thank Mihir Mahajan and David H. Nguyen for insightful comments and suggestions throughout the project. We wish to acknowledge our collaborators in the field study, Ajita John, Lynne S. Brotman and Doree Seligmann. A special thank you to Xinru Page for lending her voice for the video used in conducting the user study. This research has been supported by NSF grant nos. 0205724 and 0808783.

References

Ackerman, M. S., Cranor, L., 1999. Privacy Critics: UI Components to Safeguard Users' Privacy. In: CHI '99: CHI '99 Extended Abstracts on Human Factors in Computing Systems. ACM, New York, NY, USA, pp. 258–259.

Ackerman, M. S., Starr, B., Hindus, D., Mainwaring, S. D., 1997. Hanging on the 'Wire: A Field Study of an Audio-only Media Space. ACM Trans. Computer-Human Interaction 4 (1), 39–66.

Adams, A., 1999. Users' Perception of Privacy in Multimedia Communication. In: CHI '99: CHI '99 Extended Abstracts on Human Factors in Computing Systems. ACM, New York, NY, USA, pp. 53–54.

Adams, A., Sasse, M. A., 1999. 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.

Appelt, W., 1999. 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. Springer-Verlag, London, UK, pp. 66–78.

Begole, J. B., Tang, J. C., Smith, R. B., Yankelovich, N., 2002. Work Rhythms: Analyzing Visualizations of Awareness Histories of Distributed Groups. In: CSCW '02: Proceedings of the 2002 ACM Conference on Computer Supported Cooperative Work. ACM, New York, NY, USA, pp. 334–343.

Bellotti, V., Sellen, A., 1993. Design for Privacy in Ubiquitous Computing Environments. In: ECSCW '93: Proceedings of the Third European Conference on Computer-Supported Cooperative Work. Kluwer Academic Publishers, Norwell, MA, USA, pp. 77–92.

Borisov, N., Goldberg, I., Brewer, E., 2004. Off-the-record Communication, or, Why Not to Use PGP. In: WPES '04: Proceedings of the 2004 ACM Workshop on Privacy in the Electronic Society. ACM Press, New York, NY, USA, pp. 77–84.

Boyle, M., Edwards, C., Greenberg, S., 2000. The Effects of Filtered Video on Awareness and Privacy. In: CSCW '00: Proceedings of the 2000 ACM Conference on Computer Supported Cooperative Work. ACM, New York, NY, USA, pp. 1–10.

Business Wire, October 2008. Self-Destructing SMS Text Messaging Application for Blackberry Phones Available from BigString Corporation http://news.bbc.co.uk/2/hi/technology/4524770.stm.

Calore, M., September 2006. Privacy Fears Shock Facebook. Wired News http://www.wired.com/science/discoveries/news/2006/09/71739.

Cheng, L.-T., Hupfer, S., Ross, S., Patterson, J., 2003. Jazzing up Eclipse with Collaborative Tools. In: Eclipse '03: Proceedings of the 2003 OOPSLA Workshop on Eclipse Technology eXchange. ACM Press, New York, NY, USA, pp. 45–49.

Consolvo, S., Smith, I. E., Matthews, T., LaMarca, A., Tabert, J., Powledge, P., 2005. 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. ACM, New York, NY, USA, pp. 81–90.

Cranor, L., Dobbs, B., Egelman, S., Hogben, G., Humphrey, J., Langheinrich, M., Marchiori, M., Presler-Marshall, M., Reagle, J., Schunter, M., Stampley, D. A., Wenning, R., 2006. The Platform for Privacy Preferences 1.1 (P3P1.1) Specification. Tech. rep., W3C Working Group Note, http://www.w3.org/TR/P3P11/.

Dourish, P., 1993. Culture And Control In A Media Space. In: ECSCW '93: Proceedings of the Third European Conference on Computer-Supported Cooperative Work. Kluwer Academic Publishers, Norwell, MA, USA, pp. 125–137.

Dourish, P., Anderson, K., 2005. Privacy, security... and risk and danger and secrecy and trust and identity and morality and power: Understanding collective information practices. Tech. Rep. UCI-ISR-05-1, Institute for Software Research, University of California, Irvine.

Edwards, W. K., 1996. Policies and Roles in Collaborative Applications. In: CSCW '96: Proceedings of the 1996 ACM Conference on Computer Supported Cooperative Work. ACM, New York, NY, USA, pp. 11–20.

Gaver, W., Moran, T., MacLean, A., Lövstrand, L., Dourish, P., Carter, K., Buxton, W., 1992. Realizing a Video Environment: EuroPARC's RAVE System. In: CHI '92: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, New York, NY, USA, pp. 27–35.

Grinter, R. E., Palen, L., 2002. Instant Messaging in Teen Life. In: CSCW '02: Proceedings of the 2002 ACM Conference on Computer Supported Cooperative Work. ACM, New York, NY, USA, pp. 21–30.

Gross, T., Wirsam, W., Graether, W., 2003. AwarenessMaps: Visualizing Awareness in Shared Workspaces. In: CHI '03: CHI '03 Extended Abstracts on Human Factors in Computing Systems. ACM, New York, NY, USA, pp. 784–785.

Herbsleb, J. D., Atkins, D. L., Boyer, D. G., Handel, M., Finholt, T. A., 2002. Introducing Instant Messaging and Chat in the Workplace. In: CHI '02: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, New York, NY, USA, pp. 171–178.

Hong, J. I., Ng, J. D., Lederer, S., Landay, J. A., 2004. Privacy Risk Models for Designing Privacy-Sensitive Ubiquitous Computing Systems. In: DIS '04: Proceedings of the 2004 Conference on Designing Interactive Systems.

ACM Press, New York, NY, USA, pp. 91–100.

Huberman, B. A., Adar, E., Fine, L. R., 2005. Valuating Privacy. IEEE Security and Privacy 3 (5), 22–25.

Hudson, S. E., Smith, I., 1996. 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. ACM, New York, NY, USA, pp. 248–257.

Iachello, G., Abowd, G. D., 2005. 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. ACM Press, New York, NY, USA, pp. 91–100.

Isaacs, E., Walendowski, A., Ranganathan, D., 2002. Mobile Instant Messaging through Hubbub. Communications of the ACM 45 (9), 68–72.

Khan, R. M., Khan, M. A., 2007. Academic Sojourners, Culture Shock and Intercultural Adaptation: A Trend Analysis. Studies About Languages (10), 38–46.

Kobsa, A., Patil, S., Meyer, B., 2010. Privacy in Instant Messaging: An Impression Management Model. (Under Review).

Kobsa, A., Teltzrow, M., 2005. Contextualized Communication of Privacy Practices and Personalization Benefits: Impacts on Users' Data Sharing and Purchase Behavior. In: Martin, D., Serjantov, A. (Eds.), Privacy Enhancing Technologies: Fourth International Workshop, PET 2004. Springer, pp. 329–343, DOI 10.1007/11423409_21.

Kraut, R., Egido, C., Galegher, J., 1988. Patterns of Contact and Communication in Scientific Research Collaboration. In: CSCW '88: Proceedings of the 1988 ACM Conference on Computer-Supported Cooperative Work. ACM Press, New York, NY, USA, pp. 1–12.

Landesberg, M. K., Levin, T. M., Curtin, C. G., Lev, O., June 1998. Privacy Online: A Report to Congress. Tech. rep., Federal Trade Commission, http://www.ftc.gov/reports/privacy3/priv-23a.pdf.

Langheinrich, M., 2001. Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems. In: UbiComp '01: Proceedings of the 3rd International Conference on Ubiquitous Computing. Springer-Verlag, London, UK, pp. 273–291.

Lau, T., Etzioni, O., Weld, D. S., 1999. Privacy Interfaces For Information Management. Communications of the ACM 42 (10), 88–94.

Leary, M. R., 1996. Self-Presentation: Impression Management and Interpersonal Behavior. Westwood Press, Norwood, MA.

Lederer, S., Hong, J., Dey, A. K., Landay, J., 2004. Personal Privacy through Understanding and Action: Five Pitfalls for Designers. Personal Ubiquitous Computing 8 (6), 440–454.

Lederer, S., Mankoff, J., Dey, A. K., 2003a. Who Wants to Know What When? Privacy Preference Determinants in Ubiquitous Computing. In: CHI '03: CHI '03 Extended Abstracts on Human Factors in Computing Systems. ACM, New York, NY, USA, pp. 724–725.

Lederer, S., Mankoff, J., Dey, A. K., Beckmann, C., 2003b. Managing Personal Information Disclosure in Ubiquitous Computing Environments. Technical Report, Computer Science Division, University of California, Berkeley UCB-CSD-03-1257.

Lee, A., Girgensohn, A., Schlueter, K., 1997. NYNEX Portholes: Initial User Reactions and Redesign Implications. In: GROUP '97: Proceedings of the International ACM SIGGROUP Conference on Supporting Group Work. ACM, New York, NY, USA, pp. 385–394.

Loo, A., 2008. The Myths and Truths of Wireless Security. Communications of the ACM 51 (2), 66–71, DOI 10.1145/1314215.1314227.

Mantei, M. M., Baecker, R. M., Sellen, A. J., Buxton, W. A. S., Milligan, T., Wellman, B., 1991. Experiences in the Use of a Media Space. In: CHI '91: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM Press, New York, NY, USA, pp. 203–208.

Nardi, B. A., Whittaker, S., Bradner, E., 2000. Interaction and Outeraction: Instant Messaging in Action. In: CSCW '00: Proceedings of the 2000 ACM Conference on Computer Supported Cooperative Work. ACM, New York, NY, USA, pp. 79–88.

Olson, J. S., Grudin, J., Horvitz, E., 2005. A Study of Preferences for Sharing and Privacy. In: CHI '05: CHI '05 Extended Abstracts on Human Factors in Computing Systems. ACM, New York, NY, USA, pp. 1985–1988.

Olson, J. S., Teasley, S., 1996. 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. ACM, New York, NY, USA, pp. 419–427.

Palen, L., 1999. Social, Individual and Technological Issues for Groupware Calendar Systems. In: CHI '99: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, New York, NY, USA, pp. 17–24.

Palen, L., Dourish, P., 2003. Unpacking "Privacy" for a Networked World. In: CHI '03: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, New York, NY, USA, pp. 129–136.

Patil, S., Kobsa, A., 2004. Instant Messaging and Privacy. In: Proceedings of HCI 2004. pp. 85–88, http://www.ics.uci.edu/˜kobsa/papers/2004-HCI-kobsa.pdf.

Patil, S., Kobsa, A., 2005a. Privacy in Collaboration: Managing Impression. In: The First International Conference on Online Communities and Social Computing. http://www.ics.uci.edu/˜kobsa/papers/2005-ICOCSC-kobsa.pdf.

Patil, S., Kobsa, A., 2005b. Uncovering Privacy Attitudes and Practices in Instant Messaging. In: GROUP '05: Proceedings of the 2005 International ACM SIGGROUP Conference on Supporting Group Work. ACM, New York, NY, USA, pp. 109–112, DOI 10.1145/1099203.1099220.

Patil, S., Lai, J., 2005. 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. ACM, New

York, NY, USA, pp. 101–110, DOI 10.1145/1054972.1054987.

Smith, H. J., Milberg, S. J., Burke, S. J., 1996. Information Privacy: Measuring Individuals' Concerns about Organizational Practices. MIS Quarterly 20 (2), 167–196.

Wickramasuriya, J., Datt, M., Mehrotra, S., Venkatasubramanian, N., 2004. Privacy Protecting Data Collection in Media Spaces. In: MULTIMEDIA '04: Proceedings of the 12th Annual ACM International Conference on Multimedia. ACM, New York, NY, USA, pp. 48–55.