RC23360 (W0410-019) October 1, 2004
Computer Science

IBM Research Report

Who Gets to Know What When: Configuring Privacy Permissions in an Awareness Application

Sameer Patil, Jennifer C. Lai
IBM Research Division
Thomas J. Watson Research Center
P.O. Box 704
Yorktown Heights, NY 10598

Research Division
Almaden - Austin - Beijing - Haifa - India - T. J. Watson - Tokyo - Zurich

Who Gets to Know What When: Configuring Privacy Permissions in an Awareness Application

ABSTRACT

We report on a study (N=36) of user preferences for managing the trade-off between awareness and privacy. Participants defined permissions for the sharing of their location, availability, calendar information and instant messaging data. The context for the study was an application called mySpace, an interactive visualization of the physical workplace that provides dynamically updated information about people, places and equipment within the workplace. Findings indicate an overwhelming preference towards managing privacy by defining permissions at the group level. While family members receive among the highest levels of disclosure, interestingly, team members are granted similar levels of trust while at work during business hours. Contrary to expectations, we found that presenting participants with a detailed list of all the personal information that the system has access to did not cause participants to define more conservative awareness settings. While location proved to be the most sensitive aspect of the awareness data, participants showed high levels of comfort with disclosing room-level information at work with their team members.

Author Keywords

Context-aware computing, privacy, awareness, permission structures, contextual communication, information disclosure

ACM Classification Keywords

H5.2. Information Interfaces and Presentation: User Interfaces.

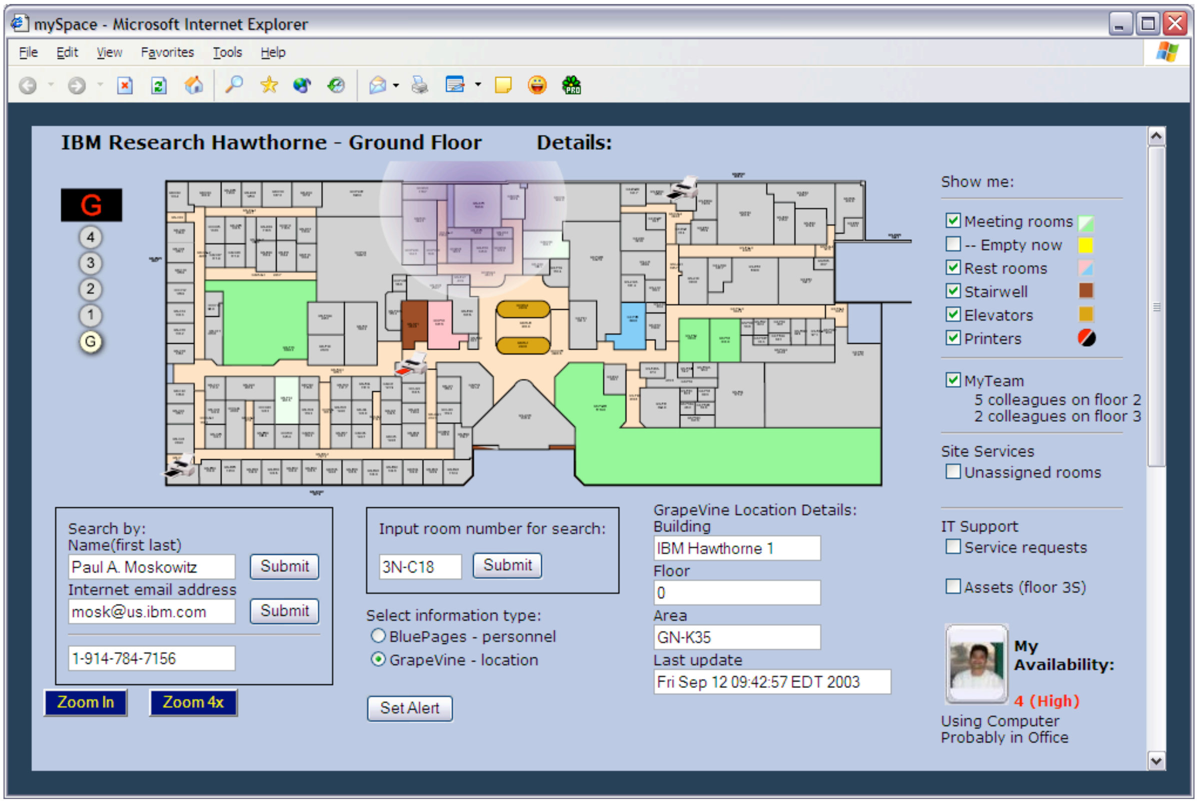
INTRODUCTION AND MOTIVATION

Understanding the impact of using technology to support communication and awareness among team members is an important field of research in both the CHI and CSCW communities. Since the early research into Media Spaces (e.g. [2, 5]) to the more recent work on sharing awareness through hand-held devices [22], the tension between privacy and awareness has existed. Researchers have examined ways to preserve privacy while sharing context by reducing the visibility of images from streaming video (e.g., shadow-views [12]), replacing video with iconic presence indicators (e.g., [7]) or replacing audio feeds with analogous sounds [19].

Our research into the privacy/awareness tradeoff has been motivated by an interest in supporting mobile workers and creating workspaces that enable distributed teams to collaborate and communicate as well as co-located ones do. mySpace is an interactive visualization of the physical workspace (usually at the building level) designed to promote awareness of the activities and availability of co-workers. Like other applications of this type, it inherently raises issues of privacy. However, while people have an interest in preserving their privacy, they also are interested in disclosing the right amount of contextual information to colleagues so that it facilitates smoother communication and enables the job they need to do.

Most awareness applications have some kind of permission structures that allow users a degree of control over the information that is available about them (e.g. in AOL Instant Messenger one can "allow users to see how long I've been idle"). However most of these involve either global permission settings applying to all users, or permissions that have to be defined on person-by-person basis. Additionally, circumstances may change such that permissions defined for a colleague yesterday (for example, if collaborating closely on a task) could no longer be applicable today. Continuous adjustments to reveal adequate information to the appropriate people at the right times becomes problematic in the digital domain. This is partly due to the difficulty in explicitly specifying preferences and partly due to the overhead of modifying settings according to context.

This paper presents mySpace, along with the results of a study that examines how users define permissions for such an application. The goal of mySpace is to support the communication and collaboration needs of workers; locally mobile ones as well as workers who travel to the different buildings where a corporation does business, and those who occasionally telecommute. The goal of the study was to


mySpace - Microsoft Internet Explorer
File Edit View Favorites Tools Help
IBM Research Hawthorne - Ground Floor
Details:
G
4
3
2
1
G
Submit
Submit
Submit
Zoom In
Zoom 4x
Set Alert

Search by:
Name(first last)
Paul A. Moskowitz
Internet email address
mosk@us.ibm.com
1-914-784-7156

Input room number for search:
3N-C18

Select information type:
○ BluePages - personnel
● GrapeVine - location

GrapeVine Location Details:
Building
IBM Hawthorne 1
Floor
0
Area
GN-K35
Last update
Fri Sep 12 09:42:57 EDT 2003

Show me:
☑ Meeting rooms 🟩
□ -- Empty now 🟨
☑ Rest rooms
☑ Stairwell 🟫
☑ Elevators 🟧
☑ Printers

☑ MyTeam
5 colleagues on floor 2
2 colleagues on floor 3

Site Services
□ Unassigned rooms

IT Support
□ Service requests

□ Assets (floor 3S)

My Availability:
4 (High)
Using Computer
Probably in Office

Figure 1. mySpace displaying the current location of a colleague

understand the type of default permissions that would allow users to operate comfortably with the level of awareness information that is available through mySpace. The study had the additional goal of understanding the boundaries of the comfort level (e.g. what type of information can be disclosed when working from home and to whom), and the impact of greater system disclosure and feedback.

MYSPACE

mySpace (see Figure 1) is a web-based interactive visualization of a user's physical workplace that provides dynamically updated information about people, places and assets. It is implemented as a portal, with users either logging on or having their login information stored as a cookie on their machine. In this way it can provide personalized access to content and applications. When a user logs on, the information associated with the profile for that user id is loaded. This can include the applications that he/she needs access to, the user's office location and the names of colleagues that the user has defined in his/her "team". The definition of team is not hierarchical, but represents the co-workers that the user selected as people he/she works frequently with. For each person in the team there is a set of permissions granted to the user. For example, if Sally has Paul in her team list, Sally will be able to view whatever information Paul has granted her permission to view. Possible permissions can include whether the phone if off the hook, the location of the wireless access point (802.11) that Paul's laptop is connected to at work, whether he is connected remotely (if not in the building), which application he is currently using, and his instant messaging status (active or away). Additionally, a badge-based location tracking system is in the pipeline. Paul can grant the full set of permissions or just a subset of them.

mySpace provides a single point of access for users who need to interact with building services (e.g. book a conference room), communicate with colleagues or view data from various databases. In Figure 1 we see that the user has requested to view the location of a colleague, Paul, and mySpace is indicating that Paul's laptop is currently connected in the area close to conference room GN-K35. Again, the user can see this information because Paul has granted permission either to this user explicitly, or has set his default permissions so that anybody running the application can see Paul's location. Had the user selected "BluePages – personnel" for the type of information instead of "Grapevine – location" mySpace would have highlighted the location of Paul's office along with his telephone number. Additionally in Figure 1, we see that the user has asked the application to highlight the location of meeting rooms, stairwells, elevators and printers. The color coding to the right of the resource list can be identified by mouse-over, and corresponds to private or public for conference rooms, color or black & white for printers, Women's or Men's for restrooms.

mySpace allows users to view the location of fixed resources (e.g. conference rooms, printers), mobile assets (e.g. laptops) and to interact with them. So for example, once a user has located the closest printer to his current location, clicking on the printer will take him to the web page that will allow him to download the driver for that particular printer. Clicking on an unoccupied conference room connects the user to the reservation page for that room, and clicking on a colleague will bring up that person's e-card [20]. An e-card (see Figure 2) is a means of initiating one-click communication with a colleague.

Communication Channels

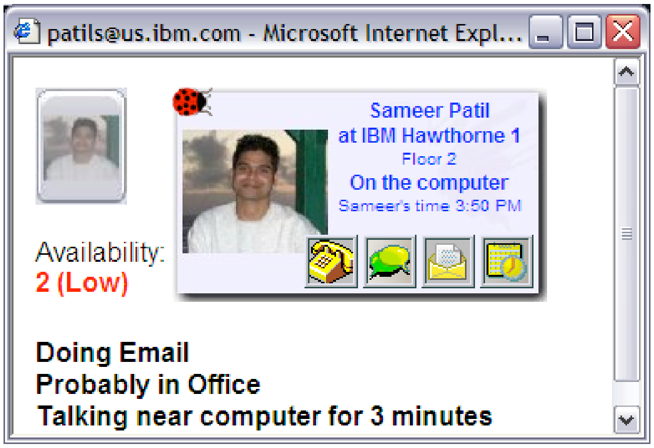
The e-card provides access to co-workers via phone, instant messaging, or email. Alternatively face-to-face meeting time can be requested via the calendar. Email support is provided by spawning a mail client, and instant messaging support is provided by programmatically starting a chat session with the selected person. Phone support is provided by a server that stores phone numbers for people and locations. When a caller initiates a phone call to a callee, the server uses the location of the caller (e.g. home or office) to determine an appropriate phone number, calls the caller, and waits for the caller to answer the call. The server then uses the callee's location to call the callee at an appropriate phone number and finally connects the two calls.

Contextual Information

MySpace uses speech detection, location, computer activity, and calendar entries to model the user's availability. For a description of how the information from these sensors was implemented see [4]. Context is shared by a background process on a person's computer, so it is available even if a person does not currently have their mySpace client up and running. MySpace uses wired and wireless network connectivity to estimate location. If a person is currently on a virtual private network or dial-up connection, "remotely connected" is displayed below their image. The person is labeled "probably in office" if he/she is connected to the local network from the access point that the person uses most often. If not connected, or if a person's computer has been idle for a long period of time, a "probably not available" label is shown. MySpace uses a set of rules and sensor data to calculate availability on a scale of one to four, with a 1 representing highly unavailable and a 4 representing highly available. The way the level is calculated is presented in [4]. When people are highly available (level 4) their image is shown in full color and their image becomes progressively greyer as their availability for communication goes down.

PRIOR WORK

Researchers in the CSCW and Ubiquitous Computing fields have been studying collaborative awareness and communication systems for more than a decade. Examples of such systems include location-tracking systems with Active Badges [23], Media Spaces [2,5], shared calendars [18] and document repositories [16]. More recently Instant Messaging (IM)-based systems [10] are becoming more pervasive and share a basic level of awareness. While researchers have recognized and studied the privacy issues involved in most of these systems, dealing with these issues is often left as an open question or future work.



Sameer Patil
at IBM Hawthorne 1
Floor 2
On the computer
Sameer's time 3:50 PM

Availability:
2 (Low)

Doing Email
Probably in Office
Talking near computer for 3 minutes

Figure 2. e-card showing context with one-click communication links

Some solutions proposed for addressing these privacy issues include distortion of information [1], context sensitive system adaptation [12], feedback loops [12], and mechanisms for access control [16]. However, most of these explorations typically involve a single aspect (e.g. video) of awareness. Additionally, the focus is often on global optimization - finding the most suitable solution to apply to the system as a whole. For example, a video-based system may allow the user to choose between blurring or pixelating the video, and the extent of the distortion. However, the user is unable to specify that they would like to send blurred video to team members, and pixilated video to managers. Moreover, the general emphasis is on letting the system manage the privacy-awareness tradeoff via automatic action(s) without explicit user involvement. While this can be quite useful in removing the burden from the user it also has the potential for leaving the user feeling disempowered.

It is well-established that individuals may be willing to give up privacy if provided with the appropriate incentives. Success of an awareness system is thus directly related to providing appropriate incentive structures [8]. However, preferences regarding when and where one might choose to reveal which aspect of privacy-sensitive information to whom and to what extent, has not yet been systematically studied.

Lederer et. al.'s study [14] of managing personal information disclosure in a ubiquitous computing environment aims at gauging the effectiveness of manual configuration of preferences by users. In an evaluation of the system with five undergraduate students at Berkeley they found that manual configuration by users was superior to settings created automatically through simple configuration rules. Despite the limitations of the study it is one of the few in the literature that systematically examines permission structures in an awareness application. In our study, we report on a larger and more diverse sample of 36 users. We also focus our attention on supporting activities in the workplace.

STUDY

In order to better understand how people might achieve an appropriate balance between awareness and privacy when using mySpace, we devised a study which required people to configure permissions for the disclosure of their personal information. We were primarily interested in exploring two aspects:

1. extracting commonality (if any) in how people configure privacy settings for an awareness application and contextual communication client in a workplace setting;
2. examining the impact of disclosing a detailed list of all personal information about the user that the system had access to.

We hypothesized that seeing a rather formidable list of personal information (see Figure X) would cause users to define more conservative permissions settings (less sharing/ more privacy). We further hypothesized that if the system provided explicit feedback regarding which aspects of a user's context were viewable by whom, users would feel comfortable enough to define permission settings that allowed greater disclosure.

Participants

Participants were recruited by requesting volunteers among permanent employees and summer interns in the research division of a large corporation. We specifically added summer interns in order to increase the variability of our user sample, as we expected interns to be younger and most likely less ingrained in the "organizational culture". Given that mySpace is a system designed for supporting collaboration in the context the workplace, our sample of users is representative of the target audience for systems such as mySpace.

A total of 36 participants took part in the study – 24 permanent employees and 12 interns. 11 out of 12 interns were between 20-30 years old, while only 2 permanent employees were younger than 30. The overall age distribution was 36% between 20-30, 25% between 31-40, 17% between 41-50 and 22% between 51-60. Participants were informed that we were studying a system called mySpace but were not told that we were explicitly looking at privacy aspects in order to not bias their perceptions regarding these aspects of mySpace. The study took about 45 minutes to complete and each participant was provided with a lunch voucher to the company cafeteria as a token of appreciation for their participation.

Methodology

The study itself consisted of three main parts with one of the authors acting as the experimenter.

Part 1 - Demonstrating mySpace:

In the first part, the participant was shown a demonstration of mySpace, highlighting its various features and illustrating different tasks that could be performed with it. In particular, participants were shown how to interpret various aspects of the user interface, how to use the system to find information about the location, availability and activities of collaborators, as well as how to set alerts to be notified of events of interest (e.g. alert me when Paul returns to his office). The same demonstration script was followed for all participants.

Part 2 – Performing tasks:

After the participant had been introduced to mySpace, we asked him or her to perform a set of 10 tasks to acquire first-hand experience with the application and to highlight its benefits in the daily work context. This also (indirectly) exposed them to any privacy implications associated with using mySpace. The tasks were identical for all participants. We selected tasks that are representative of typical situations encountered at work.

We felt that understanding the potential awareness benefits that can be derived from using mySpace provided an incentive for participants to appropriately manage the trade-off between revealing information about themselves, and preserving personal privacy. As participants were performing these tasks, the experimenter sat next to them and helped with the interface and interaction as necessary. Since none of the participants had ever used mySpace before, being able to communicate with the experimenter while performing the tasks was essential to ensure that participants achieved a sufficient level of first-hand experience with the application. At the end of each task, participants were required to write down the answer to the task, which was checked by the experimenter before proceeding.

Part 3 – Configuring mySpace:

Once participants had successfully completed all tasks, we asked them to configure permissions for mySpace according to their preferences (without explicitly mentioning that the permissions were related to privacy). Participants were told that mySpace could be configured in one of four modes: Global, Team, Groups, and Individuals. They were provided with descriptions of each mode (as shown in Table 1), and were asked to choose the mode which best fits their needs and practices.

Once they had chosen a mode, participants worked on their own to configure the permissions for mySpace. The permissions related to location, calendar, instant messaging, and availability for communication. For each of these, participants could choose one of four settings – corresponding to none, binary, coarse or fine (see Table 2).

Mode	Description
Global	One set of global permissions applies for everyone in the organization.
Team	You can define a special group of individuals called “My Team”, to which you may add any individuals you desire. You can then specify one set of permissions for the “My Team” group, and another one for the rest in the organization.
Groups	You can group individuals into various groups (e.g. Project X members, Managers, Carpool, Friends, Family), and then specify a set of permissions for each group.
Individuals	You can specify a set of permissions for each individual separately.

Table 1. Descriptions of mySpace configuration modes

Participants were asked to configure permissions while at work and while working from home. For each of these locations permissions were further subdivided into business hours and non-business hours (i.e. evenings, weekends, and holidays). As part of the existing corporate culture, remaining at work after business hours, or working from home is not uncommon.

	None	Binary	Coarse	Fine
Value	1	2	3	4
Loc.	No info	Building	Floor	Room
Cal.	No info	Busy / Not busy	Titles	Activity details
IM	No info	Online / Offline	Status msg.	Activity details
Avail.	No info	Avail. / Not avail.	Scale (1-4)	Activity details

Table 2. Permission settings in mySpace

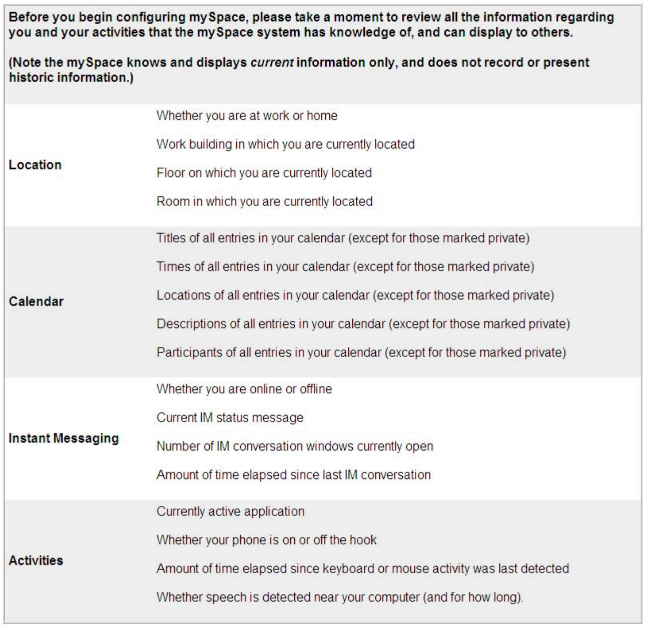
Participants who picked the Global mode were asked to configure a single set of permissions for everyone within the organization, while those who picked the Team mode were asked to configure a set of permissions for their team, and another for everyone else in the company. Participants who picked the Group mode were asked to define up to 10 groups. After specifying the groups, they proceeded to configure permissions for each group. The default was to not provide any information about the user to anyone not explicitly in a group. The Individuals mode was similar to Groups, except with individuals instead of groups although no participant selected this mode.

After configuring the permissions, participants completed an online questionnaire with questions aimed at gauging inherent attitudes towards privacy and trust. We selected questions from previous questionnaires on privacy [3,9] and trust [13, 21]. The questionnaire also gathered feedback regarding privacy attitudes towards mySpace along with demographic information. At the end of the study, the experimenter asked the participants to briefly comment on their configuration activity, and probed them regarding their choice of configuration mode.

Study conditions:

As mentioned earlier, we were interested in studying the impact of having the system explicitly disclose the information that it had access to for that user, and of providing a feedback loop confirming for the user what access had been granted to whom. To measure these effects, we defined three different conditions for the study:

- *No disclosure, No feedback*: In this condition, participants had no explicit disclosure of the information the system has access to, nor were they shown any feedback/confirmation regarding the permissions structures they had just defined.
- *Disclosure but No feedback*: In this condition, before the start of the configuration activity, participants were shown a list of all aspects of personal information that the system has access to (see Figure 3). However, they did not receive any feedback/confirmation after configuring the permissions.



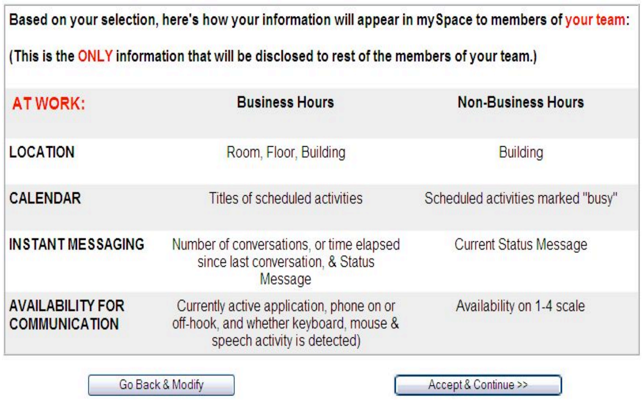
Before you begin configuring mySpace, please take a moment to review all the information regarding you and your activities that the mySpace system has knowledge of, and can display to others.

(Note the mySpace knows and displays *current* information only, and does not record or present historic information.)

Location	Whether you are at work or home Work building in which you are currently located Floor on which you are currently located Room in which you are currently located
Calendar	Titles of all entries in your calendar (except for those marked private) Times of all entries in your calendar (except for those marked private) Locations of all entries in your calendar (except for those marked private) Descriptions of all entries in your calendar (except for those marked private) Participants of all entries in your calendar (except for those marked private)
Instant Messaging	Whether you are online or offline Current IM status message Number of IM conversation windows currently open Amount of time elapsed since last IM conversation
Activities	Currently active application Whether your phone is on or off the hook Amount of time elapsed since keyboard or mouse activity was last detected Whether speech is detected near your computer (and for how long).

Figure 3. Detailed list of personal information available to mySpace

- *Disclosure and feedback*: In this condition, before the start of the configuration activity, participants were shown a list of all aspects of personal information that the system has access to.. Additionally, after they completed each configuration screen, they were shown an additional feedback screen (see Figure 4) that confirmed how the permissions they had configured would result in different aspects of their information being available to others.



Based on your selection, here's how your information will appear in mySpace to members of your team:

(This is the ONLY information that will be disclosed to rest of the members of your team.)

AT WORK:	Business Hours	Non-Business Hours
LOCATION	Room, Floor, Building	Building
CALENDAR	Titles of scheduled activities	Scheduled activities marked "busy"
INSTANT MESSAGING	Number of conversations, or time elapsed since last conversation, & Status Message	Current Status Message
AVAILABILITY FOR COMMUNICATION	Currently active application, phone on or off-hook, and whether keyboard, mouse & speech activity is detected)	Availability on 1-4 scale

Figure 4. Feedback and confirmation of configuration

Participants were randomly assigned to one of the three conditions. We did control to make sure there was an approximately even distribution of regular male employees, regular female employees, male summer interns and female summer interns assigned to each condition. Of the 36 participants we had 12 in condition 1, 13 in condition 2, and 11 in condition 3. Only the third part of the study (configuration of permissions) varied by condition, with the first two parts being identical for everyone.

FINDINGS

Our main findings indicate that majority of users would prefer the ability to specify permissions at the group level. For the most part, the permissions granted for different groups are significantly different from each other. Even though location is treated as the most sensitive information, participants are quite willing to disclose it to their team members while at work during business hours. In general, participants desire more privacy after business hours – even in an organization with a culture of flexible work hours and occasional telecommuting. Finally, disclosing all personal information that the system has access to does not seem to cause users to behave in a more privacy-preserving manner.

Preference for groups:

There was an overwhelming preference for managing permissions at the group level with 25 of the 36 participants choosing to configure permissions with the Group mode. Nine participants picked Team mode and the remaining two picked Global. Additionally, three of the nine participants who picked Team indicated that in actual use they would have picked Groups. Their choice of Team mode was driven by the fact that this mode involved less time and effort to complete the study (since it is basically a subset of Groups with just two groups: Team and the Rest of the Company).

Based on participant feedback, the preference for Groups seems to be driven primarily by the fact that it provides enough flexibility for controlling access to personal information, without requiring too much effort to set up. Participants indicated that the Global and Team modes weren't flexible enough, while the Individuals mode required more detail than necessary. Participants also mentioned that if necessary, a group with only one individual could be created. Many of those who chose Groups indicated that they organized their instant messaging contact list into groups as well. However, even participants who did not group their instant messaging contacts, chose to use Groups for mySpace because of the greater sensitivity of information involved.

The 25 participants who defined groups specified an average of 4 groups with the minimum being 2 and the maximum 5. Mode number of groups was also 4, with 15 participants who created 4 groups. We believe that in actual use, without the burden of having to specify all the groups at once, the number of groups created would probably be slightly higher than in the study condition. In general we found a lot of commonality among the group definitions, with groups being defined in a concentric circle pattern with less and less awareness being granted as one moved away from the center of the circle. In some case the center was family and in others it was team.

In order to compare user permissions across groups, the group labels created by participants were coded independently by the two authors into the following categories: team, family, friends, collaborators/department, managers, others, and rest of the people in the organization. In majority of cases, the coding was quite straightforward as participants used labels such as "My Team", or "Family Members". In the rest of the cases, knowledge of the organization was used to appropriately classify labels such as "Social Computing Group", or "Rendezvous project". For participants who did not explicitly create a group for the rest of the people in the organization (from now on referred to simply as "Rest"), we added this group for comparison purposes since participants were informed that anyone not explicitly included in a group received no awareness information (the default setting). Additionally, participants who picked the Team mode were treated as having two groups – Team, and Rest. Lastly, participants who picked the global mode were treated as having only one group, i.e. Rest. .

After this reorganization, we ended up with a mapping of all 36 participants in the group mode and groups labels coded as described earlier. The findings that follow are based on analysis of this data. In the study, for reasons of consistency and simplicity, we had asked participants to configure calendar permissions based on their location and the time (i.e. for when they were at home or at work, or during working-hours or after-hours). However, with calendar entries, the sensitivity is associated with the time of the calendar entry and as such we have excluded calendar permissions from our analyses. Additionally, although mySpace currently has no knowledge of a user's exact location within the home (it only knows whether or not the user is connected remotely), participants who inquired about the capabilities were told to not concern themselves about current limitations of the system when configuring location permissions for the home.

Permissions between groups:

We found many statistically significant differences in the permission structures granted to the distinct groups. In particular, we found that regardless of time and place, the group Rest was granted significantly lower disclosure when compared to other groups. The means for disclosure for all three aspects of awareness (location, availability and IM) ranged between 1 (none) to 2 (low). Not surprisingly, the family group received high levels of disclosure regardless of place or time with means for disclosure ranging between 3 (medium) and 4 (high) for all aspects of awareness (refer Table 2 for descriptions of values). Most interestingly, during business hours the Team group was granted the same level of awareness as family members (see Table 3). The only exception is for location awareness when working from home, where participants were willing to share with team members the fact they are at home (i.e. building-level location information) but not information at the floor or room level.

	Location		IM		Availability	
	W	H	W	H	W	H
Team (N = 33)	3.76	2.00	3.12	3.15	3.27	3.09
Fam (N = 13)	3.54	3.08	3.08	3.23	3.23	3.23
p	0.19	0.002	0.55	0.75	0.22	0.55

Table 3. A comparison of means for permission levels granted to Team and Family groups during business hours

Permissions for business and non-business hours:

As can be expected, we found that more privacy is required during non-business hours compared to business hours – both at work as well as home (with the exception of family). Compared to corresponding permissions for business hours, all groups get lower disclosure during non-business hours with the exception of family. Figures 5 and 6 show comparative mean permissions for working-hours and after-hours for location information while at work, and availability disclosure while working from home. As can be seen, disclosure for team members, collaborators, and managers decreases significantly during non-business hours. Identical patterns are seen for all aspects of awareness, regardless of whether at work or home.

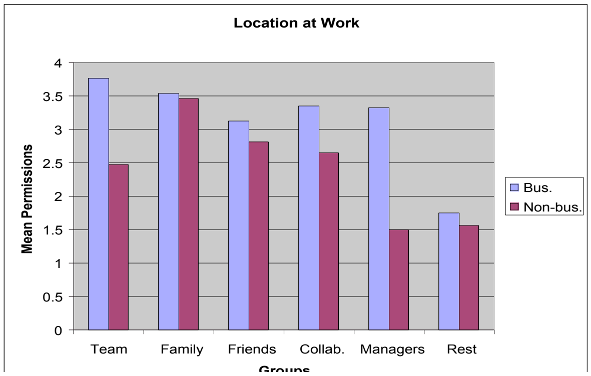


Figure 5. Comparison of means for permission levels granted to groups for location information while at work

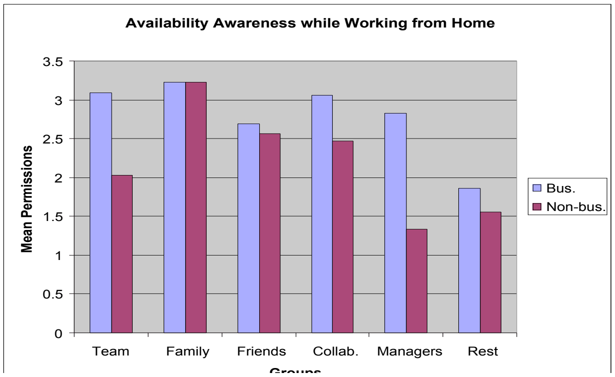


Figure 6. Comparison of means for permissions granted to groups for availability awareness when working from home

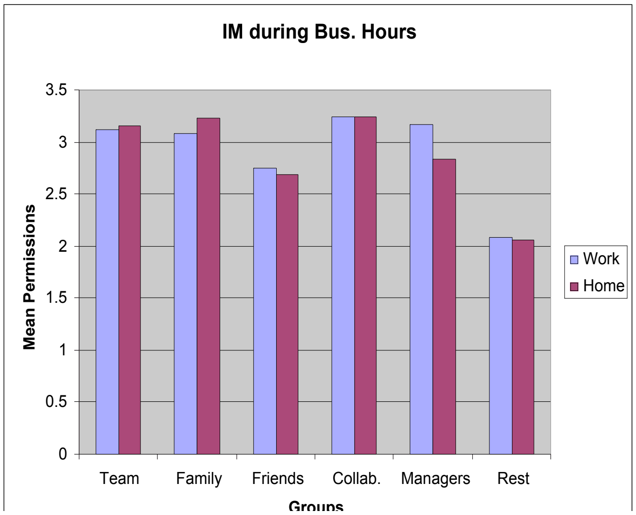


Figure 7. Comparison of means for permissions granted to groups for IM during business hours

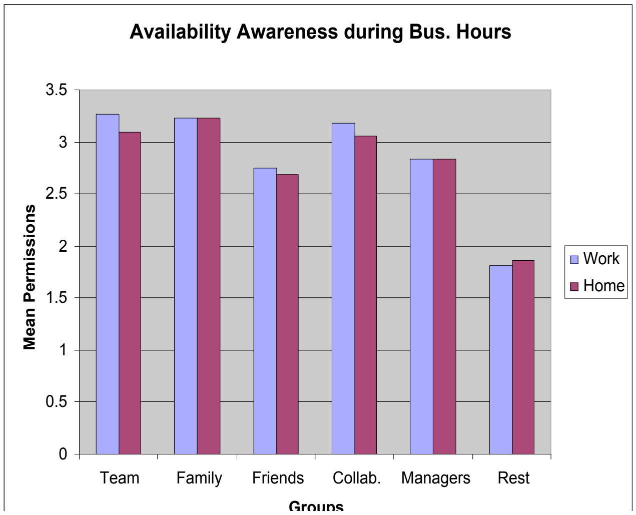


Figure 8. Comparison of means for permissions granted to groups for availability awareness during business hours

Permissions for work and home:

While levels of awareness disclosure were sensitive to time of day, place of work (either office or home) did not have a big impact. Figure 7 shows Instant Messaging awareness at home and at the office and Figure 8 shows availability for the same. Additionally disclosure for IM awareness was high even for groups far from the core center (e.g. collaborators).

The one aspect of awareness that is extremely sensitive to work place is location. Not surprisingly, people are a lot more reluctant to disclose details of their location at home, whether during or after business hours.

Variable sensitivity for various aspects of awareness:

Different aspects of personal information are sensitive to different extent [6]. Amongst the aspects of awareness that mySpace deals with, location seems to be the most sensitive, while Instant Messaging seems to be the least sensitive. This is evident from relatively large differences in permissions for location based on both time of day and work place (see Figure 9 and 10). Permissions for IM, on the other hand, remain constant and at high levels of disclosure.

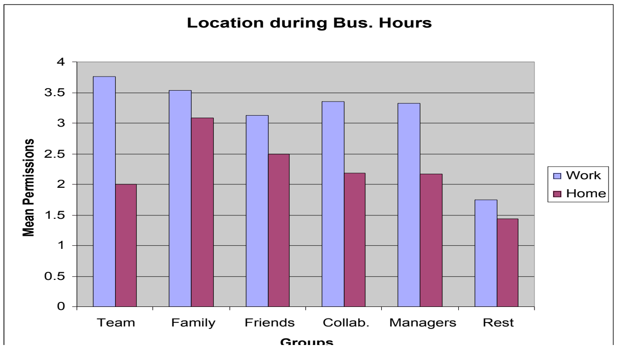


Figure 9. Comparison of means for permissions granted to groups for location during business hours

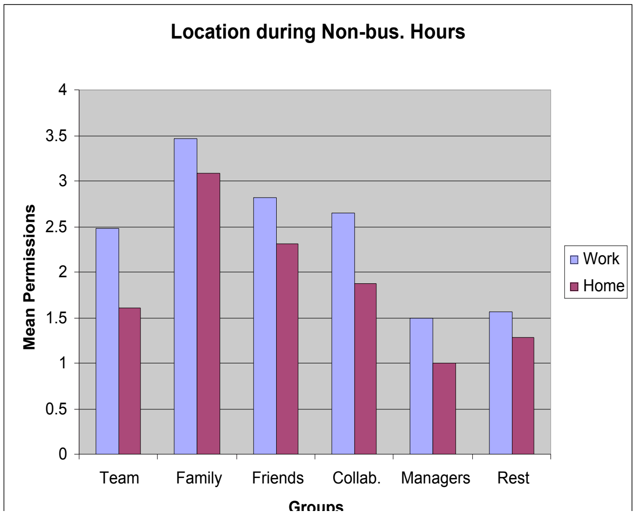


Figure 10. Comparison of means for permissions granted to groups for location during non-business hours

Effect of system disclosure and feedback:

Contrary to our hypothesis, we found that disclosing a detailed list of all the personal information that mySpace has access to does not lead participants to choose more conservative settings. A t-test between Condition 1 (no disclosure) and Condition 2 (with disclosure) revealed no statistically significant differences between permissions in most cases. The exception is when disclosing availability awareness to team members during business hours. In this case, we were surprised to see that participants tended to disclose more information whether at work (Condition 2 M=3.64, Condition 1 M=2.73, $p < 0.005$) or while working from home (Condition 2 M=3.36, Condition 1 M = 2.55, $p < 0.005$). As stated earlier, not all participants created the same number of groups. For instance, while almost every participant had a "team" group, only six created a "manager" group. It is likely that a larger sample size would lead to statistically significant differences in other factors. Several factors such as availability permissions for friends, IM permissions for collaborators were nearing statistical significance ($p > 0.05$ but $p < 0.1$) for higher disclosure in condition 2.

We had expected that permissions would move towards greater awareness disclosure in condition 3 (both system disclosure and feedback) than in condition 2. However, there were no significant differences between mean permission levels in conditions 2 and 3. The lack of statistical significance may be due to the small sample size for some of the groups (e.g. only 6 participants defined a Manager group), or it could be due to the fact that the feedback was provided *after* participants defined permission settings. Real-time feedback with a visual component may have created a more significant impact.

Inherent Privacy Preferences:

Based on participants' answers to the privacy and trust scale questions, we calculated a privacy index for each participant. The scaled responses to each question were normalized on a 0-1 scale and averaged to yield a privacy index for each participant. There was not a great range of variability among our participants regarding inherent privacy and trust attitudes. The privacy index ranges from 0.52 to 0.87. Thus all of our participants can be considered "privacy pragmatists" [2]. There were no significant differences in permission configurations based on the privacy index of the participants. Nor was there any significant impact due to organizational culture. We looked for differences between regular employees or summer interns, and again found nothing of interest except for summer interns tending to disclose less about availability to managers when at work after business hours ($p \sim 0.001$). Finally, we did not detect any major effects based on gender or nationality.

IMPLICATIONS FOR DESIGN

Our findings provide strong support in favor of providing grouping functionality in awareness systems for more than mere organizational purposes. Allowing users to define permissions at the group level appears to provide them with the flexibility they need to appropriately manage the balance between awareness and privacy, without undue burden. The burden of configuration could be further reduced by providing templates of settings for commonly used groups such as Team, Collaborators, or Family. Defaults for these templates could be determined relatively easily with a quick user study of the target population (or defaults could be based on our findings if working in a similar environment). Creating defaults that are an acceptable starting point for most individuals avoid the pitfall of requiring too much configuration [15]. Even if only 75-80% of the defaults are appropriate for the user/group combination, it makes it much more likely that the user will fine-tune the remaining 20-25%. Since the majority of users rarely take the time to modify default settings, getting the defaults right is not only critical for avoiding too much configuration but also to provide a balanced privacy-awareness setting. Setting defaults to broadcast more awareness information than necessary can undermine individual privacy, and may lead to underutilization (or even abandonment) of the system. On the other hand, creating defaults with higher privacy settings than required by the average comfort level could undermine the group awareness benefits of the system.

Many participants in our study expressed the desire to have the ability to copy the settings from another group, and make changes to that copy. Having a global template that groups can inherit from, or having the functionality to copy the settings from a pre-existing group also seem like useful functionalities for reducing the configuration burden without forfeiting flexibility. Also, automatic (or semi-automatic) adjustment of settings to accommodate differences in preferences for business and non-business hours could help the user to achieve a comfort level between awareness and privacy.

While it is not surprising that users were very sensitive to location information being broadcast from their home, system builders of location-aware systems will be heartened by the finding that users are not averse to sharing location information with their team during working hours. The mode permission for team members during business hours is 4, i.e. room-level location information - the highest possible awareness setting for location. If system builders can provide for greater user control over more sensitive aspects of location awareness, users may feel comfortable enough to disclose this type of information.

There is also a case to be made for not excluding family and friends from consideration even when building systems primarily designed to support the workplace. Apart from the obvious case of employees having family and friends working at the same organization, there also seems to be a general desire to have a small extension of "home" into daily work life by allowing family and friends to have at least some access to oneself even when at work. Of all participants who chose the group mode of configuration, more than 50% (13/25) chose to create a group for family, while more than 60% (16/25) chose to create a group for friends. (It is quite possible that some of the others may also have wanted to create these groups, but may not have done so due to the assumption that mySpace was only designed for the employees of the organization.) The question of how exactly non-organizational personnel can be incorporated in a workplace system is one open to further research.

It is quite encouraging that disclosing a detailed list of personally sensitive information collected by the system, does not seem to scare users into choosing more privacy-conservative settings. In fact, it appears as if, at least for some factors, such a disclosure acts as a trust-builder, reassuring users to reveal more information to the colleagues on their team [17]. The table-based confirmation feedback interface that we designed to further help users overcome privacy concerns, seems not to have been effective enough to achieve this purpose. However, a feedback mechanism that operates concurrently with the configuration activity and provides a quick visual overview of which aspects of awareness are made available by the system to whom, seems worth exploring.

Finally, the willingness of participants to disclose relatively higher levels of information about their IM activities can be leveraged by embedding IM within other systems. An example is disclosing IM status on a person's page in the directory. There are many organizations in which use of IM is either completely prohibited, or severely restricted. These organizations can probably benefit by promoting an organizational culture in which use of IM is encouraged, rather than prohibited

CONCLUSION

A study of how users specify permissions for disclosing various aspects of awareness about themselves reveals a strong desire to manage privacy at the level of groups.

Empowering users to control how and when aspects of awareness information regarding themselves is disclosed by the system to whom, can enable them to find more suitable points of balance between awareness and privacy. This is evident from the willingness of participants to provide high levels of awareness to team members while at work during business hours. Disclosing upfront the details of personal information that a system deals with seems to act as a trust builder. Appropriate feedback mechanisms and interfaces need to be explored for further helping users visualize their permission settings.

ACKNOWLEDGMENTS

We would like to thank (anonymized), the creator of the e-card and the associated communication infrastructure, (anonymized) the brains behind the implementation of mySpace, as well as all the participants in our study. We also acknowledge anonymized, anonymized, and anonymized for their help with various aspects of the study.

REFERENCES

1. Boyle, M., Edwards, C, and Greenberg, S. (2000) The Effects of Filtered Video on Awareness and Privacy. In Proc. CSCW 2000.
2. Bly, S.A., Harrison, S.R. and Irwin, S. (1993) Media Spaces: Bringing People Together in a Video, Audio, and Computing Environment. Communications of the ACM, 36 (1), pp. 28-46.
3. Cranor L. F., Reagle J., and Ackerman M. S. (1999) Beyond concern: Understanding net users' attitudes about online privacy. AT&T Labs Research Technical Report TR 99.4.3, http://www.research.att.com/projects/privacystudy/
4. Fogarty, J., Lai, J., and Christensen, J. (2004) Presence and Availability in a Context Aware Communication Client. In International Journal of Human Computer Studies (2004)
5. Gaver, W., Moran, T., MacLean, A., Lövstrand, L., Dourish, P., Carter, K. and Buxton, W. (1992) Realizing a Video Environment: EuroPARC's RAVE System. In Proc. CHI 1992, pp. 27-35.
6. Goffman, Erving, (1959) The Presentation of Self in Everday Life, Doubleday.
7. Greenburg, S. (1996) Peepholes: Low Cost Awareness of one's Community. In Conf. Companion CHI 1996, pp.206-207.
8. Grudin, J. (1988) Why CSCW Applications Fail: Problems in the Design and Evaluation of Organizational Interfaces. In Proc. CSCW 1988.
9. Harris, L. & Associates and Westin A. F. Westin (1998) E-commerce & Privacy: What Net Users Want. Privacy & American Business, Hackensack, NJ
10. Herbsleb, J. D., Atkins, D. L., Boyer, D. G., Handel, M. and Finholt T. A. Introducing Instant Messaging and Chat in the Workplace. In *Proc. CHI 2002*, pp. 171-178.
11. Hindus, D., Ackerman, M. S. et al. (1996) Thunderwire: A Field Study of an Audio-only Media Space. In Proc. CSCW 1996.
12. Hudson, S.E. and Smith, I. (1996) Techniques for Addressing Fundamental Privacy and Disruption Tradeoffs in Awareness Support Systems. In Proc. CSCW 1996, pp. 248-257.
13. Jarvenpaa, S.L., Leidner, D. (1998) Communication and Trust in Global Virtual Teams. Journal of Computer Mediated Communication, 3, http://www.ascusc.org/jcmc/vol3/issue4/jarvenpaa.html
14. Lederer, S., Beckmann, C., Dey, A. K. and Mankoff, J. (2003) Managing Personal Information Disclosure in Ubiquitous Computing Environments. University of California, Berkeley, Computer Science Division Technical Report UCB-CSD-03-1257.
15. Lederer, S, Hong, J. I., Dey A. K., and Landay, J. A. (2004) Personal Privacy through Understanding and Action: Five Pitfalls for Designers. Personal and Ubiquitous Computing, special issue on Privacy and Security for Ubiquitous Computing (to appear).
16. Mark, G., Fuchs, L. et al. (1997) Supporting Groupware Conventions through Contextual Awareness. In Proc. ECSCW 1997.
17. Moore, D. A., Kurtzberg, T. R., Thompson, L. L., and Morris, M. W. (1999) Long and short routes to success in electronically mediated negotiations: Group affiliations and good vibrations. Organizational Behavior and Human Decision Processes,77, 1, pp. 22-43.
18. Palen, L. (1999) Social, Individual & Technological Issues for Groupware Calendar Systems. In Proc. CHI 1999, pp. 17-24.
19. Smith, I. and Hudson, S.E. (1995) Low Disturbance Audio for Awareness and Privacy in Media Space Applications. In Proc. Multimedia 1995, pp. 91-97.
20. Richards, J. and Christensen J. (2004) People in our software. ACM Queue, Feb. 2004.
21. Rotter, J. (1967) A new scale for the measurement of interpersonal trust. Journal of Personality, 35, pp. 615-665.
22. Tang, J., Yankelovich, N., Begole, J., Van Kleek, M., and Li, F. (2001) ConNexus to Awarenex: Extending Awareness to Mobile Users. In Proc. CHI 2001, ACM Press, pp. 221-228.
23. Want, R., Hopper, A. et al. (1992) The Active Badge Location System. ACM Transactions on Information Systems (TOIS), 10(1), pp. 91-102.

Contribution and Benefits Statement:

We present overwhelming evidence for user preference for managing privacy at the group level. Users are quite willing to disclose location information to team members during business hours at work.