UNIVERSITY OF CALIFORNIA,
IRVINE

# Reconciling Privacy and Awareness in Loosely Coupled Collaboration

DISSERTATION

submitted in partial satisfaction of the requirements
for the degree of

DOCTOR OF PHILOSOPHY

in Information and Computer Sciences

by

Sameer Patil

Dissertation Committee:
Professor Alfred Kobsa, Chair
Professor Bonnie Nardi
Professor Alladi Venkatesh

2009

# DEDICATION

**TO MY MOTHER,** Sulabha Patil, who made countless sacrifices for my success
**TO MY FATHER,** Ajit Patil, who encouraged me to broaden my horizons
**TO MY SISTER,** Swati Patil, who supported me unconditionally
**TO MY ADVISOR,** Alfred Kobsa, who turned me from a student into a scientist

# TABLE OF CONTENTS

# LIST OF FIGURES

# LIST OF TABLES

# ACKNOWLEDGMENTS

I would like to thank all collaborators in the various research projects that have been included in this thesis: Lynne S. Brotman, Ajita John, Jennifer Lai, Bertolt Meyer, and Doree Seligmann. I also acknowledge the help of Jeff Elliott, Xinru Page, and Heather Pulliam in conducting some of the studies, and the support of Hadar Ziv in the implementation of our design ideas into a prototype system. I am grateful for the insightful comments of Mihir Mahajan and David H. Nguyen that have helped improve this thesis.

This research has been supported by NSF grant nos. 0205724 and 0808783.

# CURRICULUM VITAE

## Sameer Patil

### EDUCATION

**Doctor of Philosophy in Information and Computer Sciences** **2009**
University of California, Irvine *Irvine, California*

**Master of Science in Computer Science & Engineering** **2001**
University of Michigan, Ann Arbor *Ann Arbor, Michigan*

**Master of Science in Information** **2001**
University of Michigan, Ann Arbor *Ann Arbor, Michigan*

**Bachelor of Engineering in Electronics Engineering** **1998**
University of Bombay *Bombay, India*

# ABSTRACT OF THE DISSERTATION

Reconciling Privacy and Awareness
in Loosely Coupled Collaboration

By

Sameer Patil

Doctor of Philosophy in Information and Computer Sciences

University of California, Irvine, 2009

Professor Alfred Kobsa, Chair

Awareness of the activities of one's collaborators is crucial for effective and efficient collaboration. In loosely coupled collaborations, particularly those distributed across time and distance, such awareness is impoverished. Interpersonal Awareness and Interactions Systems (IAIS) aim to foster awareness and overcome the impoverishment. Promoting awareness, however, is in tension with the individuals' desire for privacy. We explored how the privacy-sensitivity of IAIS can be improved by empowering the users to reconcile privacy desires with awareness needs. Our investigation started with Instant Messaging (IM) as a representative case of IAIS and expanded to a corporate awareness application that incorporates multiple aspects of awareness. Finally, we engaged in a field study of a large, geographically distributed software development project to broaden our scope to the entire ecology of IAIS utilized in loosely coupled collaboration. We show that the desire for impression management is an underlying cause of the desire for privacy in technology-mediated interpersonal interactions – both directly as well as indirectly via a causal link with the desire for visibility (to oneself) of one's IAIS-projected impression. We also provide a framework that describes how privacy management in loosely coupled collaboration operates. The framework lists important situational characteristics (viz., issues, relationships,

temporality, technology, and space) and interpretive influences (viz., self, team, site, organization, and cultural environment) that are grounded in our data. Further, we identify differences in interpersonal privacy concerns among collaborators in the U.S. and India and describe five factors that lead to the observed differences: physical characteristics of the workplace, nature of interpersonal relationships, conceptualization of privacy, intra-team competition, and management style and hierarchy. The research generated several design suggestions for improving the reconciliation of privacy and awareness in IAIS. We describe the prototype we implemented to demonstrate the designs. Specifically, the prototype adds the functionalities of notice, negotiation, control over conversation archives, expiration of contacts, encryption of channels and archives, visualization of collective activities, and group-level preference specification. Users concur that our enhancements provide improved support for privacy management.

# Chapter 1

# Introduction and Motivation

## 1.1 Introduction

Today, high-speed network infrastructure allows collaborative work to span distance and time. Project teams in many organizations comprise of employees spread across continents. Scientists and engineers engage in global research initiatives in order to take advantage of specialized instruments, expertise, and/or data collection opportunities that may be spread throughout the world. Full or partial telecommuting provides people with increased flexibility to balance work needs with domestic responsibilities. When collaborators are distributed geographically (Kraut et al., 1988; Olson and Olson, 2000) and/or temporally (Pankoke-Babatz and Syri, 1997), their awareness of each others activities, routines, tasks, and availability tends to be substantially reduced. Yet, such awareness is essential for efficiency and effectiveness of collaborative work (Hudson and Smith, 1996; Prinz et al., 1998; Neale et al., 2004).

This impoverishment of awareness in distributed collaboration has been long recognized by researchers in the field of Computer Supported Collaborative Work (CSCW).

Various Interpersonal Awareness and Interaction Systems (IAIS) have been built to compensate for this impoverishment by enabling greater interaction among collaborators and by disseminating information that fosters awareness. These include:

- Systems with the specific goal of making collaborators more aware of each others activities (e.g., video or audio media spaces (Bly et al., 1993; Hindus et al., 1996), location tracking systems (Want et al., 1992), Instant Messaging (IM) (Nardi et al., 2000; Herbsleb et al., 2002), chat (Bradner et al., 1998), and blogs (West et al., 2005)).

- Single-user systems augmented to include awareness features in order to facilitate collaboration (e.g., word processors (Cadiz et al., 2000), calendars (Palen, 1999), and programming environments (Cheng et al., 2003)).

- Community-driven systems that provide awareness mechanisms for opportunistic social discovery (e.g., social bookmarking (Millen et al., 2006), and music sharing (Voida et al., 2005)).

- Infrastructures that seamlessly and automatically capture, store, process and disseminate awareness information in domains such as workplaces (Yan and Selker, 2000), hospitals (Bardram, 2004; Black et al., 2004), conference centers (Dey et al., 1999), and homes (Kidd et al., 1999).

## 1.2 Motivation

In promoting awareness, IAIS face a tension with an individuals desire for privacy (Hudson and Smith, 1996). This interaction between awareness and privacy is not limited to IAIS but is a characteristic of everyday life. Westin (1967) describes it as a balancing act:

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

As Schwartz (1968) notes:

> "We are led to relinquish our private information and activities by the expediencies and reciprocities routinely called for in daily life. We all know, for example, that in order to employ others as resources it is necessary to reveal to them something of ourselves."

Normally, individuals perform this balancing act by utilizing the spatial and architectural features of the environment (Schwartz, 1968) (e.g., a door), biological and cognitive features of humans (Westin, 1967) (e.g., limitations of human memory), and shared understanding of norms (Westin, 1967). Privacy is managed (relatively seamlessly) based on the familiarity with these aspects through the extensive experience of conducting daily affairs. This does not imply that privacy violations do not occur in familiar everyday settings. In fact, privacy violations due to accidental disclosure are not uncommon (Schwartz, 1968). For instance, situations in which familiarity with aspects of day-to-day affairs breaks down (e.g., moving to another country) have been observed to be particularly problematic for privacy management. However, when a violation of privacy does occur, and is detected, individuals typically engage in social negotiation until a commonly agreed upon (or comfortable) state of privacy is reached for everyone involved. Westin (1967) describes social practices such as covering the face, averting the eyes, and facing the wall. As Palen and Dourish (2003) point out, "Privacy is understood to be under continuous negotiation and management, with the boundary that distinguishes privacy and publicity refined according to circumstance."

In case of IAIS, this balancing act involves reconciling the desire to reap the benefits of awareness for improving the effectiveness of collaboration on one hand, and the desire to maintain individual privacy on the other hand. Notably, these systems move the practices of reconciling privacy and awareness from the largely familiar physical domain to the relatively new digital domain (Agre and Rotenberg, 1997). As mentioned above, situations in which familiarity breaks down are problematic for privacy management, and may lead to privacy violations. Shifting the operation of privacy management to the digital domain poses precisely such difficulties.

Certain characteristics of the digital domain differ substantially from the physical world, namely high-speed transmission, potential persistence, enhanced computation,

and disembodiment (Heath and Luff, 1991) and dissociation (Bellotti, 1997) of interaction. Due to these distinguishing characteristics, the transformation of expectations and behaviors from the physical to the digital world is not always effective and/or possible. On the one hand, these characteristics can inhibit behaviors that may be fluid and seamless in the social realm. Here privacy runs into the social-technical gap – "the divide between what we know we must support socially and what we can support technically" (Ackerman, 2000). On the other hand, characteristics of the digital domain enable actions that may otherwise be impossible or prohibitively difficult to achieve socially. Lessig (1999) sums this up rather nicely: "In the 1790s the technology was humans; now it is machines. Then the technology noticed only what was different; now it notices any transaction. Then the default was that searchable records were not collected; now the default is that all monitoring produces searchable records. These differences add up."

As a result, effectively reconciling both privacy and awareness needs of collaborators poses a significant challenge for the designers of IAIS built for supporting collaboration. Insufficient attention to this reconciliation is a factor potent enough to undermine the system. If users are unable to reconcile awareness needs and privacy desires seamlessly, the system fails to achieve its full potential. For instance, Lee et al. (1997) found that when privacy was desired users of their Portholes video system preferred simply to turn off their cameras because it was cumbersome to fiddle with other privacy options such as blurring the video. Herbsleb et al. (2002)faced hurdles in the adoption of their chat system because initially the default settings were too private. The system required significant initial setup effort from the users in order to provide awareness benefits. In our own research, we have found that users who were forced to use IM because of organizational requirements often used circumvention tactics. They set their status to "away" or "busy," or, conversely, changed defaults to always appear online even when they were away from their desks (Patil and Kobsa, 2004,

2005a). Such circumvention results in suboptimal productivity gains.

Focusing on awareness and paying insufficient attention to privacy aspects may evoke strong user backlash. This is illustrated by the recent example of new privacy-invasive awareness features introduced by the popular social networking site Facebook (http://www.facebook.com). Facebook introduced a new awareness feature that automatically presented a person with an aggregation of every single activity of their friends. Hundreds of thousands of users were outraged. The user revolt ranged from online petitions and protest groups to threats of a boycott (Calore, 2006). Facebook eventually apologized and introduced privacy controls for these newsfeeds (Zuckerberg, 2006).

Clearly, user opposition due to privacy concerns can translate into minimal use or abandonment of a system. If this were to happen, organizations stand to lose their investment in collaborative technology. Moreover, organizations that design and build these systems, as well as their customers, face the prospect of longer-term damage as their trust and credibility is lowered in the opinions of their users (Adams, 1999; Adams and Sasse, 1999).

To avoid these problems, IAIS need to be sensitive to the privacy concerns of their users. Improving the privacy-sensitivity of IAIS by empowering their users to reconcile their privacy desires with the needs of awareness serves as the motivation of our research.

# Chapter 2

# Related Work

We first provide an overview of the conceptual foundations of privacy. We then discuss related work from the literature regarding privacy aspects of IAIS. Finally, we point out the gaps in prior research that our investigations attempt to fill.

## 2.1 Privacy

The notion of privacy has recently received enormous attention both in the scientific literature and in the popular press. Figure 2.1 shows the number of non-fiction books and articles with "privacy" in their titles that have been published since 1960[1]. Of the about 21,000 publications, nearly two-thirds have been published in the past ten years alone. This dramatic rise in the research productivity from the mid-1990s onwards coincides with the advent of the World Wide Web and e-Commerce. The small peak in the 1970s corresponds with the global induction of data processing into businesses

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

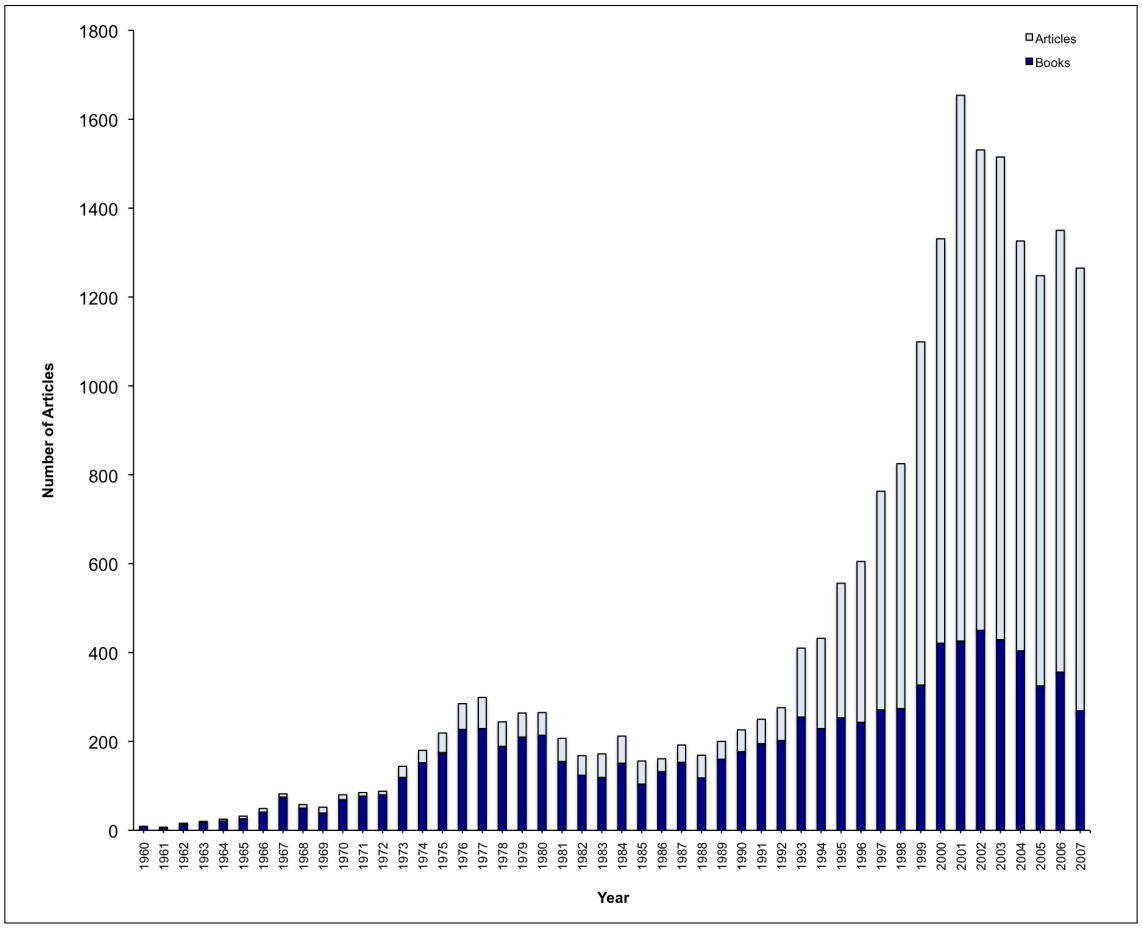


Figure 2.1: WorldCat non-fiction books and articles with "privacy" in the title

and government administration. (Both of these changes engendered widespread privacy concerns, and led to privacy legislation in some parts of the world). To some extent, the rapid increase of research articles as opposed to books mirrors the scientific disciplines in which privacy research takes place. While privacy research originated in the fields of law, psychology, sociology, communications, political science, architecture, and urban design, it has since expanded into the computer and information sciences, organization and management research, economics, and the health sciences.

The concept of privacy is so intricate that there is no universal definition of it. The difficulty of defining privacy stems from its highly *situated* and context-dependent nature. Even in the same situation, different individuals may have differing opin-

Table 2.1: Three perspectives regarding the concept of privacy

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

ions and expectations regarding what privacy means to them. For instance, Westin (1991) classified individuals as privacy fundamentalists, pragmatists, or unconcerned based upon differences in their stated privacy preferences. This context dependency and variability between individuals make dealing with privacy a difficult task. To quote Lederer et al. (2004):

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

There are three main perspectives from which the notions of privacy are commonly described and analyzed (see Table 2.1):

**Normative:** Analyzed philosophically, privacy is an ethical concept (Negley, 1966; Johnson, 1985; Mason, 1986). Privacy is viewed as a "right" of individuals and thus as a matter of "freedom." For example, Warren and Brandeis (1890) characterized privacy as "the freedom to be left alone." From this perspective, privacy is a civil liberty that needs to be protected through legal and political means. Traditionally, the focus of privacy protection has been on laws, contracts and policies aimed at protecting the individual from large entities such as corporations and governments (Lessig, 1999). Increasingly, however, legislation is being extended to protect one's privacy from other individuals (for instance, laws against hacking, stalking or voyeurism).

**Social:** From the social perspective, privacy has psychological and cultural roots (Westin, 1967; Schwartz, 1968). Privacy is "socially constructed" based on the behavior and the interactions of individuals as they conduct their day-to-day affairs. For instance, in Goffman's (1959) analysis "the expressive component of social life has been treated as a source of impressions given to or taken by others," where expression "has been treated in terms of the communicative role it plays during social interaction." This manifests itself in Rachels' (1975) claim that "privacy is necessary if we are to maintain the variety of social relationships with other people that we want to have." Thus, managing privacy allows us to manage social relationships. Altman (1975) has described the process of privacy management as a "dialectic and dynamic boundary regulation process" – conditioned by the expectations and experiences of the parties involved and under continuous negotiation and refinement. Given the differences in norms, expectations, experiences, behaviors, and laws across cultures, it is no surprise that privacy manifests itself differently in different cultures (Westin, 1967; Milberg et al., 1995). Viewed socially, the notion of privacy evolves as external changes bring about changes in expectations and behavior and as technology introduces new forms or means of interaction.

**Technical:** The technical perspective views privacy in terms of the functional characteristics of digital systems. Discussions from this perspective tend to investigate how ethical and social considerations could be operationalized. Privacy is thus treated as the desire for selective and adequate control over data and information – both incoming and outgoing. For example, Stone et al. (1983) describe privacy as the "ability of the individual to personally control information about oneself" whereas Samarajiva (1997) extends it to the "control of outflow of information that may be of strategic or aesthetic value to the person and control of inflow of information including initiation of contact." The issues under consideration include the capture, storage, ownership, usage, and access of personal data. For instance, the code of Fair Information Practices was developed from this perspective (U.S. Department of Health Education and Welfare, 1973).

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

## 2.2 Research on Privacy in IAIS

As Figure 2.1 shows, tackling privacy issues engendered by IAIS has gained increased attention over the past decade. This research falls along three major themes: users studies of specific IAIS, design principles and guidelines derived from theoretical considerations, and privacy-enhancing technical solutions. We discuss each of these be-

low.

### 2.2.1 User Studies

Initial findings related to privacy were primarily noted "on the side" in studies aimed at evaluating experiences with the awareness aspects of systems. Dourish (1993) characterizes privacy controls along a "social-technical continuum." On the social end of this continuum, social pressures and norms are relied upon to prevent system abuse, while on its technical end, technology prevents attempted misuse. Social controls are likely to work well only within small and relatively well-knit communities (Dourish, 1993; Ackerman et al., 1997). Even in such environments with high levels of interpersonal trust, social controls may result in very strong protective behaviors such as turning the system off and altering ones work habits (Mantei et al., 1991). In contrast, technical privacy protections raise the acceptance and adoption of a system by virtue of the fact that it increases user trust that the system would protect privacy (Dourish, 1993). Later studies confirm that trust in a system is an important implicit factor in privacy assessments (Adams, 1999; Adams and Sasse, 1999). Our work (Patil and Lai, 2005)shows the importance of increased system transparency as a possible promoter of trust in the system (see Chapter 7).

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[2], partly via practices such as cryptic entries, omissions, defensive scheduling, and partly via social anonymity within the larger organizational context. Lee et al. (1997) suggest that mere existence of mechanisms to address privacy needs is not enough; these mechanisms need to be

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

lightweight. In other words, users desire mechanisms that allow them "to increase or decrease privacy, to inform other users of their new privacy state and to provide immediate feedback of the change," in a way that "facilitates the tight coupling between the means to change privacy and the means to obtain feedback that privacy is attained." As Herbsleb et al. (2002) discovered, the lack of lightweight, low-burden privacy management mechanisms increased setup time and delayed user adoption. Moreover, 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. Additionally, Nardi et al. (2000) noticed that plausible deniability of physical presence was used frequently by IM users as a means for privacy management.

Recently, studies of IAIS have started targeting privacy as the primary object of investigation. These studies have unveiled a number of factors that affect users privacy judgments. These include users relationship with the information recipient, the purpose and usage of requested information, the context, and the sensitivity of content (Adams, 1999; Adams and Sasse, 1999; Lederer et al., 2003b; Consolvo et al., 2005; Olson et al., 2005). Our work (Patil and Kobsa, 2004, 2005a,b)confirms many of the same factors and reveals additional ones such as users' understanding of how technology works (see Chapter refim). Lederer et al. (2003c) also showed that a-priori manual configuration of privacy preferences is better than automatic strategies – especially for information that users deem important.

Generic privacy attitudes and behaviors could also come into consideration in IAIS. Therefore, it is instructive to look at a few privacy studies conducted in other contexts. For instance, as mentioned above, Westin (1991) classified individuals into three main clusters – privacy fundamentalists, pragmatists, and unconcerned. This distinction may also apply to privacy concerns in the context of IAIS. Milberg et al.

(1995) and Bellman et al. (2004) reported that privacy concern varies by country. At the same time, they mentioned that "secondary use" and "improper access" rank as the top two concerns across most nationalities. Cranor et al. (1999) listed anonymity and information sensitivity as important privacy-related factors for Internet users. Finally, Fox (2000) showed that users are often ignorant of the basic concepts underlying their digital domain activities, and do not typically utilize the tools available for privacy protection.

### 2.2.2 Theories, Principles, and Guidelines

As discussed in Section 2.1, privacy is 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). Owing to this complexity, IAIS designers have found it difficult to translate the privacy-related findings of the various user studies into concrete system design guidance. Researchers have tried to address this problem by framing the theoretical insights into privacy in forms that are more amenable to system designers. For instance, Boyle and Greenberg (2005) describe a vocabulary of privacy that permits designers to discuss privacy in an unambiguous manner. To suggest ways of thinking about privacy in socio-technical environments, Palen and Dourish (2003) outline a model of privacy that is based on the theory developed by social psychologist Irwin Altman (1975; 1977). It characterizes privacy as a process that regulates the boundaries of disclosure, identity, and temporality. This process is both dynamic (i.e., shaped by personal and collective experiences and expectations) and dialectic (i.e., under continuous boundary negotiation).

Researchers in the "technology trenches" have further distilled general guidance on

privacy into specific design principles and guidelines in order to enable better privacy management. Bellotti and Sellen (1993) propose a design framework based on feedback and control regarding information capture, construction, accessibility, and purpose. In essence, feedback mechanisms aim at providing users with information that helps them make privacy judgments, and control mechanisms empower them to take appropriate actions to manage privacy. In addition, Bellotti and Sellen (1993) provide eleven criteria for evaluating design solutions – trustworthiness, appropriate timing, perceptibility, unobtrusiveness, minimal intrusiveness, fail-safety, flexibility, low effort, meaningfulness, learnability, and low cost. Langheinrich (2001) draws upon Fair Information Practices (U.S. Department of Health Education and Welfare, 1973) in proposing that privacy-sensitive systems ought to notify the user appropriately, seek consent, provide choice, allow anonymity or pseudonomity, limit scope with proximity as well as locality, ensure adequate security, and implement appropriate information access. Iachello and Abowd (2005) add the principle of proportionality – "any application, system tool, or process should balance its utility with the rights to privacy of the involved individuals." In contrast, Lederer et al. (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) further develop privacy risk models to analyze how well a system meets such principles or avoids the pitfalls. These risk models are a set of information sharing questions pertaining to the social and organizational context in which the system is situated, and the technology which is used to implement the system. Finally, to incorporate user perceptions, Adams Adams (1999) provides a privacy model based on interacting concerns of information sensitivity, information receiver and information usage.

### 2.2.3 Design Techniques

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

Several techniques have been proposed and explored for the implementation of principles and guidelines such as those described above. These include:

- encryption (Diffie and Hellman, 1979);
- 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), and grouping and templates (Olson et al., 2005; Patil and Lai, 2005);
- automatic and manual control of the granularity of disclosed information (Dourish and Bly, 1992; Lee et al., 1997; Palen, 1999; Consolvo et al., 2005);
- feedback via visualization (Gross et al., 2003), sound (Gaver et al., 1992), intelligent agents (Ackerman and Cranor, 1999), and contextualized disclosure (Kobsa and Teltzrow, 2005);
- distortion of disclosed information (Boyle et al., 2000);
- support for anonymity (or pseudonymity) (Appelt, 1999);

- inference of appropriate awareness disclosure based on modeling (Begole et al., 2002).

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

## 2.3 Gaps in Prior Research

A closer scrutiny of existing research reveals several gaps. Studying IAIS with privacy as the focus of investigation has begun only within the past few years. As a result, user experiences regarding privacy management mechanisms of IAIS could be further expanded. Various design techniques and approaches listed above have indeed provided means for reconciling privacy and awareness. However, as several studies indicate (Lee et al., 1997; Whitten and Tygar, 1999; Herbsleb et al., 2002), the success of these systems is limited unless the users can utilize these mechanisms effectively and seamlessly.

Moreover, users studies or experiments so far have concentrated on specific IAIS. Given that collaborators typically need and utilize a variety of IAIS, a broad picture of privacy management across different systems is needed. A promising approach towards this end is a field study involving individuals engaged in distributed loosely coupled collaboration. No research has reported such privacy-focused field work yet.

Although prior research draws attention to the process of privacy management and to user privacy attitudes and practices when interacting with IAIS, the motivation that underlies the privacy desires is largely unexplored. In this regard, there seems to be

merit in the interpretation of Goffman's (1959) work on impression management as an underlying cause of privacy concerns in technology-mediated interactions (Ackerman and Cranor, 1999; Lederer et al., 2003b; Boyle and Greenberg, 2005). Goffman, however, dealt only with face-to-face interactions and did not discuss the connection of impression management to privacy. Thus, empirical evidence is needed to confirm the extensibility of impression management for purposes of loosely coupled distributed collaboration. If empirically validated, focusing on impression management as the motivation behind privacy concerns could provide the means to make privacy management mechanisms more effective and seamless across a broad variety of IAIS.

Finally, it should be noted that, apart from some exceptions (e.g., (Greenberg and Rounding, 2001)), current research on privacy in IAIS is not targeted exclusively toward loosely coupled collaboration. Designers of IAIS built for this type of work must identify and support the awareness and privacy needs that arise in such collaborations.

# Chapter 3

# Research Questions and Hypotheses

As the preceding chapters highlight, what collaborators need is neither awareness nor privacy in isolation, but a contextually appropriate reconciliation between the two. Therefore, we focused on practices and preferences surrounding such reconciliation. From this focus, we formulated the following hypothesis to address the gaps in research that were identified earlier:

**H1:** In IAIS used for supporting loosely coupled collaboration, effective and seamless reconciliation of awareness needs and privacy desires could alleviate privacy concerns without unduly compromising the benefits of awareness.

In order to verify this hypothesis, we began by investigating current user preferences and practices regarding reconciliation of privacy and awareness needs in loosely coupled collaboration. Early results of these investigations suggested "impression management" as an important motivator for privacy management. This led to the

formation of our second hypothesis:

**H2:** Impression management (Goffman, 1959) is an underlying cause of privacy concerns in IAIS.

The results of the investigations undertaken to verify the above hypotheses not only served to uncover why privacy concerns arise in this context, but also highlighted the shortcomings of current IAIS systems for achieving optimal reconciliation of privacy concerns and awareness needs. We then translated this understanding into a framework that describes the process of privacy management in loosely coupled collaboration. We also designed improvements for privacy management support in IAIS and built a prototype that applies these designs to IM systems.

Specifically, we tackled the following questions:

**Q1:** What is the nature of these concerns?

**Q2:** In what ways do privacy management practices manifest themselves as collaborators interact with IAIS, and with each other, through these systems?

**Q3:** Which privacy needs do current IAIS leave unfulfilled? In particular, in what ways are current privacy management mechanisms in IAIS lacking in effectiveness and seamlessness?

**Q4:** How can privacy management in IAIS be improved?

Q1 was aimed at verifying the second hypothesis, while Q3 and Q4 were concerned with the first. Q2 served to inform both simultaneously.

# Chapter 4

# Scope

Before attempting to answer these questions, it was important to scope the investigation appropriately. This section describes the scope within which we have concentrated our research along with a discussion of why this scope is particularly fruitful for the research questions being addressed.

## 4.1 Domain of Collaboration

Collaboration occurs in a variety of domains, such as the workplace, school, home, communities etc. While there is much similarity in collaborative practices across the various domains, there are also domain-specific variations due to differences in the relationships between individuals in a given domain. At the same time, it should be noted that the exact boundaries between the domains (e.g., "home" and "work") may not always be as clear-cut today as they traditionally have been (for instance, consider the case of telecommuters). We will concentrate on collaborative practices encountered in what an individual would choose to describe as "work" – regardless

of a specific place or time at which such activity takes place.

## 4.2 Concept of Privacy

Section 2.1 described that privacy is a highly context-dependent, complex, and nuanced concept that without a universal definition (see Bellotti (1996) for a discussion of various ways in which privacy has been defined). Limiting ourselves to any particular definition of privacy, from among many, could have resulted in a characterization that is too narrow or too broad for any particular situation within the collaborative work context. To avoid this problem, in each of the studies we conducted, we allowed the study participants to define and describe privacy for themselves as they viewed it in the various situations they encountered while engaging in collaborative work. This approach allowed us to capture the diversity of views regarding privacy, and minimized the likelihood of bias being introduced by the researchers' own conceptions of privacy.

## 4.3 Concept of Awareness

Similar to privacy, awareness can also be defined broadly to include any piece of information that provides knowledge about another entity. It could then be broken down further into specific, lower-order aspects such as awareness of someone's presence or location. In our research, we utilized the notion of awareness that is of relevance to collaborative work, viz., activity awareness (Carroll et al., 2003). As Carroll et al. (2003) explain,

> "The social exchange and actions of a work group are situated in a rich

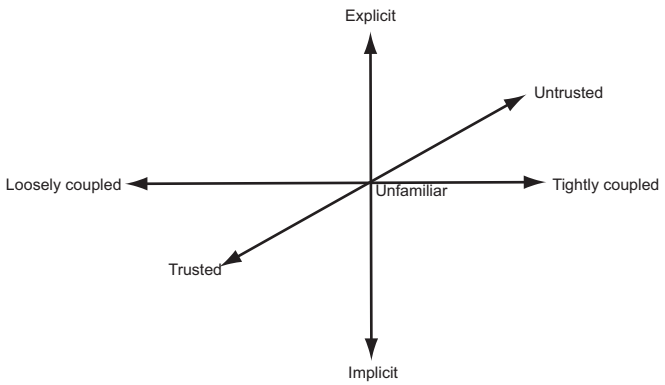


Figure 4.1: Positioning IAIS along privacy-relevant dimensions

> context of organizational strategies and objectives, job roles and responsibilities, interpersonal relationships, task assignments and interdependencies, and tool-handling and material resources. This context is the domain of activities – long-term joint endeavors directed at major goals."

Thus, activity awareness implies an awareness of other people's tasks, progress, plans, and context, and awareness of the understandings regarding the division and coordination of subtasks in service of the higher-level goal. It should be apparent that the focus is on dynamic awareness information (see Danis, 2000). Activity awareness subsumes lower-level aspects such as awareness of presence, location, interruptability etc.

## 4.4 Positioning of IAIS

In order to further focus our investigations, we positioned IAIS in a space of three independent dimensions (see Figure 4.1). These dimensions are discussed below.

### 4.4.1 Nature of Awareness Mechanisms

By their very nature, all IAIS deal with capturing, storing, analyzing, disseminating, and/or displaying awareness information in some form. However, there is a distinction to be made between systems that are built specifically for awareness purposes (e.g., (Dourish and Bly, 1992; Appelt, 1999; Cadiz et al., 2000)), and those that provide awareness implicitly by virtue of their use (Bellotti, 1996). For instance, the primary purpose of email is to communicate the content of a message. Yet, by virtue of the timestamp, IP address, server names, and other header information, email implicitly reveals awareness information. (It is also important to note that researchers have been exploring systems that could be built on top of other systems to make implicit aspects of awareness more explicit (Fisher and Dourish, 2004; Froehlich and Dourish, 2004).) Thus, IAIS can be characterized to lie along a continuum ranging from explicit to implicit awareness functionalities (see Figure 4.1). For example, a system like IM that provides communication mechanisms along with awareness (Nardi et al., 2000) could be positioned somewhere in the upper half in Figure 4.1.

Systems that deal with awareness information explicitly, try to expose the benefits of such awareness in a direct manner because provision of awareness is their primary goal. Drawing attention to the awareness feature often also has the side effect of highlighting the associated privacy issues. In contrast, when awareness is implicit or secondary to the function of a system, the attention of the user is on other (i.e., non-awareness) aspects of the primary task carried out with the system (e.g., the user is much more likely to focus on the contents of an email message rather than on the IP address from which the email is being sent). Consequently, privacy aspects typically remain invisible in such cases (Bellotti, 1996).

### 4.4.2 Activity Coupling

The user activities that IAIS support lie along a continuum from loosely to tightly coupled (Olson and Teasley, 1996; Olson and Olson, 2000; Neale et al., 2004). For instance, the work of software developers working on two separate modules of the same program may be less tightly coupled than that of a developer and a tester working on the same module. Coupling is a characteristic of the task itself and depends on how different pieces of the task are segmented among collaborators.

As Olson and Olson (2000) explained, tightly coupled activities typically require "frequent, complex communication among the group members, with short feedback loops and multiple streams of information." Therefore, when tasks are tightly coupled, it is typical that awareness of each other's activities among collaborators is improved owing to the more frequent and prolonged communication and coordination that are usually a part of carrying out the work. This, in turn, leads to the collaborators developing greater familiarity with each other, thereby further increasing awareness.

On the other hand, when collaboration is loosely coupled, the amount and frequency of coordination and communication are typically lower. This, in turn, implies less awareness information is available as a integral part of the work activities themselves. In such cases, a variety of factors may affect awareness unfavorably. These include infrequent and asynchronous interaction between collaborators, less shared context, and the involvement of the collaborators in multiple simultaneous tasks and projects (Olson and Teasley, 1996; Pinelle and Gutwin, 2003). Moreover, loosely coupled collaborations are often geographically and temporally distributed. Distribution across distance and time has an adverse effect on the availability of awareness information from sources such as peripheral vision, hallway conversations etc. (Kraut et al., 1988)

Thus, task coupling and the associated work arrangements impact awareness on two fronts:

1. **Need:** In tightly coupled work, the need for awareness is high owing to the tight coupling which requires keeping aware and in sync. In contrast, the awareness needs of loosely coupled work are typically lower and are also variable depending on the phase in the overall scheme of the work. The awareness needs may also be of different *kind*. For instance, two designers working together to sketch out a design on a whiteboard need different sorts of awareness information compared to two designers sitting next to each other but working on their own on two subparts of a larger design. In the former case, given the shared and synchronous focus on the same activity, awareness requirements involve ensuring that the collaborating parties are aware of the focus of attention of others (Dourish and Bly, 1992). In the latter case, the collaborators need awareness of the status and schedule of others.

2. **Availability:** As mentioned above, the settings and arrangements in which work is carried out are often different for loosely coupled activities compared to tightly coupled work which is often synchronous and/or co-located and/or with a shared focus of multiple collaborators on the same task. The differences in the physical settings, work times, and task division impact the amount and kinds of awareness information that is available. Moreover, as mentioned above, tighter coupling tends to result in greater communication, coordination, and interaction between the collaborating parties, which in turn tends to increase the availability of awareness information. This suggests that the richness and amounts of available awareness information are lower in loosely coupled collaboration.

It could be argued that the lower availability of awareness in the case of loosely coupled

collaborations is unproblematic because the needs of awareness are also lower. While this argument could apply to some collaborative endeavors, for many others it may not hold, because:

- The decrease in awareness availability may be greater than the corresponding decrease in awareness needs.
- On those occasions when awareness needs are greater, awareness information may still be difficult to obtain owing to the same factors that lead to lower overall awareness.
- Awareness needs cannot always be predicted accurately in advance, so collaborators may find themselves in need of awareness information at times when it is not available, or cumbersome to obtain.
- Considering only the immediate needs of the work activities ignores the role of awareness in fostering impromptu informal interactions which play an important role in improving the effectiveness of collaboration; such interactions are far less common in loosely coupled collaborations (Kraut et al., 1988).

Owing to these factors, a large majority of the IAIS for supporting loosely coupled work are designed with the aim of providing explicit support for fostering awareness.

At the same time, privacy expectations in loosely coupled activities can be expected to be greater than in the case of tightly coupled work. In fact, some of the very factors that engender impoverished awareness (viz., less frequent and asynchronous interaction, less shared context, multi-tasking etc.) also imply lower familiarity and trust among the collaborators. This may, in turn, contribute to higher desires for privacy from these colleagues. Additionally, if the work is geographically distributed across different countries, cultural differences in privacy attitudes and the laws of the

various nations may need to be taken into account (Milberg et al., 1995; Bellman et al., 2004). In contrast, tightly coupled activities typically involve synchronous, co-located, and highly focused interpersonal interactions. In such cases, one is able to monitor and manage one's privacy much more easily thereby leading to lower privacy concerns overall.

### 4.4.3 Nature of Relationships

The nature of the relationships among the various users of an IAIS forms the third dimension. These relationships can range from trusted and familiar (e.g., a colleague with whom one shares an office) to unfamiliar but known (e.g.,an employee in a different branch of the organization) to untrusted (e.g., a stranger who might read one's blog).

The degree of familiarity with the individual with whom one interacts is important in shaping attitudes and behaviors. For instance, greater familiarity reduces the importance of static awareness information (Danis, 2000) because collaborators are likely to know it, or can ask for it directly (Lederer et al., 2003a). Lederer et al. (2003a) also point out differences in privacy considerations when dealing with familiar as opposed to unfamiliar parties. While a great deal of research and legislation focuses on privacy protection from organizations and unknown people (e.g., governments, corporations, hackers, stalkers, marketers etc.), the other side of the continuum has received lesser attention. Yet, this side – ranging from the trusted to the unfamiliar – is of greater importance when dealing with IAIS.

## 4.5 Research Scope

Exploration of reconciliation of privacy and awareness needs are best served by looking at those scenarios that simultaneously exhibit significant needs for both awareness as well as privacy. Not only are such scenarios the most germane to the topic of the research, but they also facilitate investigation by making the underlying issues prominent and visible. Moreover, given the high importance of both awareness and privacy in these situations, they also present the most stringent requirements for the reconciliation of the two.

To identify the scenarios that meet this criterion, one needs to look at how awareness and privacy needs in a collaborative context are influenced by position of an IAIS in the 3-D space of Figure 4.1. Based on the above discussion on awareness and privacy considerations in IAIS, we wish to underscore the following points:

1. Given that awareness information (that is not the result of direct collaborator interaction) is typically also linked with privacy concerns, IAIS that focus on explicitly promoting awareness are also likely draw attention to the associated privacy issues.

2. Since collaborators may be assumed to have at least some level of trust and familiarity with each other, IAIS of interest in collaborative work are those that lie towards the trusted end of the relationship axis.

3. Loosely coupled collaboration may require, and derive greater benefit from, external IAIS support for fostering awareness. At the same time, privacy needs are also greater with looser coupling.

The above points serve as constraints for the Nature of awareness mechanisms, activity coupling, and nature of relationships axes in Figure 4.1 respectively. Applying

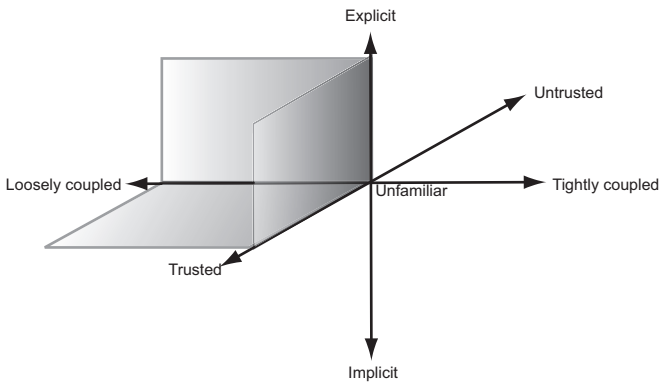


Figure 4.2: Scope of research is shown by the shaded region

these constraints identifies the shaded area as shown in Figure 4.2. We limited our research scope to IAIS that fall in this shaded area. In other words, we investigated the reconciliation of privacy and awareness needs in IAIS designed for loosely coupled collaboration among individuals who are at least somewhat familiar with each other. We anticipate that the results of the investigations will also apply to IAIS that fall in the other areas of Figure 4.2 since they pose less stringent awareness and/or privacy needs.

# Chapter 5

# Research Overview

To tackle the research questions listed in Chapter 3, we followed a mixed methodology that included both qualitative and quantitative techniques. This chapters provides an overview of our approach.

We began by examining IM as a representative case of IAIS (see Chapter 6). We chose IM because:

- IM has been growing in popularity and adoption for supporting collaborative work,
- IM falls in the shaded area in Figure 4.2, and
- Prior research on IM hinted at the presence of privacy management practices in IM usage (Nardi et al., 2000).

We first conducted semi-structured interviews with frequent IM users (Patil and Kobsa, 2004). Findings from the interviews led us to believe that impression management may be an underlying cause of privacy concerns in interpersonal interac-

tions (Patil and Kobsa, 2005a). Combining this insight with prior literature, we formulated a model that captures the relationship between privacy concerns and impression management. Further, we designed a questionnaire for broader coverage and deeper exploration of privacy issues in IM that were identified in the interviews. The questionnaire was administered online to adult IM users across the U.S. We used linear structural modeling to verify our hypothesized model using the questionnaire responses (Kobsa et al., 2010).

The findings of the above IM studies were also used to generate design ideas for improving privacy management functionalities in current IM systems. We built a prototype implementation of these design ideas as an IM plugin. User evaluation of the plugin suggests that the plugin would improve IM privacy management (Patil and Kobsa, 2010).

To expand our scope beyond a specific system, we conducted a user study of a corporate awareness application called mySpace (see Chapter 7). The mySpace application is an interactive visualization of the physical workspace. The visualization presents awareness information dynamically combined from four separate pieces: location, calendar, IM activity, and level of "busyness." We studied how users chose to manage their privacy in mySpace by looking at how they configured their privacy permissions for the various mySpace contacts. The results confirmed that several of our findings from the IM studies applied more broadly to other IAIS.

Next, we engaged in a field study of a geographically distributed collaborative project (called Project X) in a large multinational corporation (see Chapter 8). At various stages, Project X included anywhere between 80 to 130 contributors spread across five different locations: four in the U.S. (in three different time zones) and one in India. The software developed by Project X comprised eighteen interdependent modules integrated into a single release. Members of Project X utilized a plethora of systems

for communication, coordination, and awareness, making it an ideal candidate for broadening the scope of our earlier findings to cover the entire ecology of IAIS utilized in loosely coupled collaborations.

To study Project X, we used the following methods over a period of 18 months:

- Non-participant observations of the planning meetings of the Project X management team
- Semi-structured interviews with 52 Project X contributors
- Observations of workplace arrangements during visits to Project X sites
- Online questionnaire administered to all members of Project X

Findings from the field study further corroborated the generalizability of the results of our previous studies to other IAIS. The findings also contributed a framework that illustrates how the process of privacy management operates in achieving a contextually-appropriate reconciliation of privacy and awareness. We uncovered the situational characteristics and interpretive influences that are involved in the process. Further, we found that contributors in India expressed higher privacy concerns compared with those of their colleagues from the U.S. Combining the data from the field study with prior literature, we offer several explanatory factors that may contribute to the difference.

As mentioned in Section 4.2, none of the studies imposed a definition of privacy on the participants. Moreover, to avoid biasing the participants, we did not reveal our focus on studying privacy. The chapters that follow describe each of the above endeavors and provide further methodological details specific to each study. The chapters also discuss the insights gained from designing and conducting these studies.

# Chapter 6

# Instant Messaging

Having identified IM as an IAIS well-suited for an initial exploration of the research questions (see Chapter 5), we have pursued a long thread of research aimed at unpacking privacy considerations in IM. Initial exploratory interviews helped us understand the issues involved and guided the formulation of hypotheses regarding privacy attitudes and behaviors. This, in turn, guided the formation of a questionnaire that was administered online to confim the hypotheses across a wider spectrum of users. The findings of these studies were used to generate design solutions for enhancing IM privacy management, which were then implemented into a prototype packaged as an IM plugin. Finally, user evaluation of the plugin was conducted to validate its utility and identify avenues for improvement. The following sections describe each of these efforts.

## 6.1 Semi-structured Interviews

We interviewed seven frequent users of IM to understand their privacy attitudes, expectations and practices when using IM, and to see whether these differed with the location and purpose of IM usage. We solicited participants via a posting to a mailing list, as well as via word of mouth. Potential participants were sent a short (5 questions) multiple-choice screening questionnaire in order to get a sense of the IM system(s) they used, the usage frequency, and the number of contacts in their list(s).

### 6.1.1 Subjects

Seven subjects participated in the study:

- A software developer in a large corporation
- A graphic designer in the technical staff of a university
- A software engineer in a small Indian consulting firm (with offices and clients in India and the U.S.)
- A doctoral student whose native language is Spanish
- A technical support person in a large corporation
- An engineer at a large corporation that handles sensitive defense contracts
- A second-year undergraduate student studying Social Science

We deliberately chose individuals with diverse backgrounds who were involved in different types of undertakings in different types of environments, in order to compare and contrast use of IM in a broad variety of situations. Two of the subjects (graphic

designer and technical support person) were female. Subjects were between mid-20 to early 30, except for the undergraduate (20) and the engineer (above 50). All were experienced users of IM and had been using it for at least a year. All used IM from multiple locations (e.g., work, home, school), and had more than 20 people in their contact lists. The frequency of IM use varied from a few hours per month to more than 8 hours/day. Subjects participated in the study on a voluntary basis, and no compensation was provided.

### 6.1.2 Methodology

A semi-structured interview of about 1 to 1.5 hours was conducted with each subject. For the graphic designer, we did a second follow-up interview of about half an hour to probe more into some of the information provided in the first conversation. In order to get a sense for the physical environment in which the subjects use IM, we tried to conduct interviews at the place where the person used IM the most (However, three took place at different locations.) All interviews were conducted face-to-face, except for the subject from India who was interviewed by phone. The interviews were digitally tape recorded and then transcribed for analysis.

We used about 20 rather broad questions as a guideline for the semi-structured, conversational interviews. The questions were meant to gather information about people's tasks and routines, the manner in which they use IM in their daily lives, and their expectations and behavior regarding privacy – both in general and specific to IM. Questions were tailored to each subject based on their answers to the 5-question screening questionnaire. Additional questions were asked during the interview, as deemed necessary to gather relevant information.

### 6.1.3 Results

Despite the diversity of chosen subjects, their expectations and practices regarding privacy were strikingly similar. (While there also were quite a few differences, we will mostly focus on the similarities here.) In general, subjects had trouble articulating what "privacy" meant to them. They found it much easier to discuss privacy in terms of concrete situations and examples. This is to be expected, given the highly context-dependent nature of privacy.

All subjects claimed not being overly concerned with privacy when using IM. Most operated with the general assumption that they do not have much privacy when working online. Yet, as will become clear in the following discussion, quite a few of their practices suggest a definite desire and concern for privacy, despite claims to the contrary.

Overall, we found that privacy concerns of subjects fell along three main dimensions: who, when & where, and what. These are described below:

#### Who (Known vs. Unknown)

Subjects reported the desire to have a very high degree of privacy from people not on the contact list. Non-contacts were often treated as strangers with unknown intentions. Subjects took pains to make sure that anyone not on the contact lists could not see any information about them. For instance, only one subject (undergraduate student) maintained a public profile. He also indicated that many of his friends had profiles as well. We believe that this difference is most likely due to the fact that undergraduates are at an age and stage in life where they actively engage in socializing and want to "advertise" themselves.

People on the contact list, on the other hand, were treated as trusted acquaintances. Given the greatly lowered privacy barrier for contacts as opposed non-contacts, it was hardly surprising that all subjects were quite careful about whom to add to their list. The graphic designer relied upon standardized screen-name conventions followed at her workplace, the software developer used the corporate directory which was integrated with the IM client at his organization, while the doctoral student and the software engineer reported adding only those people with whom they had had extensive face-to-face relationships for some period of time.

This careful screening of contacts at the outset also resulted in relatively few contacts being blocked or deleted later. Blocking occurred either when someone was added in error, or upon some significant external change(s). For example, the software developer mentioned blocking his ex-girlfriend after they broke up. Similarly, the doctoral student mentioned deleting contacts from his old job after he quit that job.

For known contacts, subject practices pointed to a desire for different levels of availability for different groups of people – such as co-workers, family, friends. For instance, some of our subjects had reservations about having their superiors on their contact list. The doctoral student collaborated with his supervisors only via email, as he did not want to always be accessible to them via IM. This is further corroborated when subjects mentioned using IM grouping mechanism to selectively monitor their contact list.

> Graphic designer: *"The IWTT members are right here. It's the first thing that I see, and I can tell my team members are on."*
>
> Doctoral student: *"My wife logs in and only looks at the group of family members. If no one in that group is logged in she will disconnect. That's the only group of people she cares about at that time."*

### When & Where (Availability)

This dimension can also be looked at as the desire to manage availability to avoid interruption or distraction from current task. Expectations and practices regarding availability heavily depended on location, time and (work) context. Thus, subjects had different desires regarding their availability while working (from any location including their homes), as opposed to not working. ("Work" here is used in a general sense and includes schoolwork.) While working, subjects wanted to be as available as possible to co-workers for collaboration. They also paid more attention to the availability of the co-worker contacts on their list. Subjects tried to keep contacts informed of their availability via status indicators. The graphic designer left descriptive status messages even if she was away from her desk for only 5 minutes. The software developer turned off the "auto-idle" feature, because often he was around yet not using the computer, incorrectly creating the impression that he was away from his desk. The graphic designer also mentioned that she often guessed the location of her contacts based on changes in the picture or icon that they chose to associate with their name.

> Graphic designer: *"Sometimes somebody will work from home in the morning and then come in the afternoon. But the only thing that distinguishes between locations is the different icons that people might have. They might have an icon when they're at work and an icon on their home computer. And when they log in you can tell just based on an icon."*

Subjects frequently employed plausible deniability (Nardi et al., 2000) as an indication of (un)availability. They chose not to respond immediately to incoming messages if they were otherwise occupied. Similarly, a non-response to a message they initiated was taken to mean that the contact was busy and will reply at a later, more convenient

time. The software engineer, however, said that he tried to send a quick "busy right now" message whenever possible.

For subjects with working lives, IM allowed a limited extension of "home" into "work." Subjects reported having personal, non-work contacts in their list at work. However, while at work, IM conversations with friends, family, and significant others were reported to be few and far between, with primary attention being devoted to work-related matters. The occasional personal conversation seemed to serve the purpose of maintaining social bonds, and catching a moment of relief from stress of work.

Interestingly, the reverse was not typically true; "work" rarely extended into "home," unless specifically working remotely from home. Subjects made sure that work did not invade personal life. The software engineer almost never used IM from home as he wanted to "stay away from the computer." The graphic designer and the software developer had separate personal IM accounts, which they used from home, while the doctoral student piggybacked on his wife's account at home. Subjects did not have any work-related contacts in these accounts.

### What (Content)

Subjects were greatly aware of the sensitivity of the contents of their IM conversations. For the most part, IM was treated similar to email or written communication. 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 had a reasonable expectation that their conversations will only be read by the intended recipient(s). The undergraduate student believed that the chances of anyone grabbing his conversations were so miniscule that he was not concerned. Moreover, they expected the recipient(s) to follow the same common etiquette as for email if shar-

ing conversations with a third party. In fact, the graphic designer's workplace had come to an unwritten consensus about the policies to be followed for sharing saved conversations with others not part of the original conversation.

> Graphic designer: *"We created rules within our group. I work with 5 people. And the rule is, anything that is said in AIM or in email, if you want to forward it on to a third party you have to check with the person first, tell them exactly what you would be clipping and pasting and sending. If they okay it, fine. But you cannot do that under any circumstances, no matter how benign the conversation seemed. You can't do that unless you've asked first. And so we stick to that rule and have not had any problems."*

Most subjects expressed unease at the prospect of their IM conversations being saved by their contacts. However, they had resigned themselves to the fact that this was something that they could neither know about nor control. At the same time, they all cited instances in which a previously saved conversation either by them or by a contact had been useful at some later point. All seemed to employ the strategy of consciously trying to avoid saying anything over IM that might be potentially harmful for them in the future.

All subjects reported switching to a different medium of communication for conversations that they deemed too sensitive for IM. Subjects resorted to the telephone or a face-to-face conversation in such cases – either because they did not want a written record of the conversation, or because they felt that IM was too impersonal a medium, or because they felt that written communication was not the best choice for the situation, or some combination of the above reasons.

Finally, all subjects reported being aware to some extent that others who walk up to their desks were able to glance at the contents of their screens. The software developer and the software engineer said that they minimized their windows whenever someone approached their desk.

> Software developer: *"I'd rather have it minimized and blinking than there for everyone to see what I'm talking about."*

The undergraduate student also minimized windows, but only when he was conversing about the person approaching him. The doctoral student mentioned that his conversations are in Spanish, providing him with an added layer of privacy in an English-speaking country. The graphic designer as well as the doctoral student initially denied being too concerned about others watching the screen. However, further probing revealed that the doctoral student often turned off the monitor if engaged in a conversation with someone physically at his desk, while the graphic designer mentioned occasionally using the "Show Desktop" button to minimize all windows. She also recalled an instance in which she felt quite awkward when her mother was watching the screen over her shoulder.

### 6.1.4 Impression Management

In general, subjects' practices pointed to a desire for different levels of availability for different groups of people – such as co-workers, family, friends – based on their own location and (work) context. For instance, some of our subjects harbored reservations about including their superiors in their contact lists. The doctoral student collaborated with his supervisors only via email, as he did not want to always be accessible to them via IM. This is further corroborated when subjects mention using

the grouping mechanism provided by IM to selectively monitor their contact list.

> Graphic designer: *"The IWTT members are right here. It's the first thing that I see, and I can tell my team members are on."*

> Doctoral student: *"My wife logs in and only looks at the group of family members. If no one in that group is logged in she will disconnect. That's the only group of people she cares about at that time."*

Based on the above findings from the interviews, and from the work of Goffman (1959) regarding face-to-face interactions, it seemed to us that privacy expectations and behaviors in IAIS are primarily shaped by the desire to control and shape how one appears to others, i.e., the wish to project an appropriate impression of oneself through the system to the various parties involved. As Palen and Dourish (2003) point out, "We seek to maintain not just a personal life, but also a public face. Managing privacy means paying attention to both of these desires."

This may be seen in the subjects' practices of presenting themselves differently by being "available" to different extent to different groups of people. Subjects' wish to control sharing of their one-on-one conversations (with any party not part of the original conversation) also pointed to their desire for being in command of the impression they project about themselves to the third party in question. The impression that users wished to present to someone seems dependent on the type of relationship with the person. The impression one would want to project to one's superior was quite different from that one would want to project to peers. Providing information to trusted colleagues raised fewer privacy concerns than to unknown third parties. This is highlighted in the interviews by the subjects' very strong desire for privacy from people not on their contact lists. The particular practices that people employ

to manage their impression on others seemed to be influenced by a variety of factors such as system defaults, personal preferences, prior knowledge and experiences, group norms, organizational policies, and cultural expectations.

The desire to manage one's impression is likely to strongly influence how privacy and awareness needs are reconciled. One is likely to demand more privacy in matters that could potentially reflect poorly upon oneself. On the other hand, one may tolerate, or even demand, less privacy when the situation creates a favorable impression of oneself from the point of view of others. For example, due to a general fear of monitoring, employees may be reluctant to distribute records of the exact time at which they arrive at work every day. However, an employee who consistently comes in early may in fact wish to have this fact known widely as a testimony of greater commitment to work. People regularly try to gauge the impression that others form of them (especially in groups and organizations), and, at times, aim to influence it through a variety of means (Giacalone and Rosenfeld, 1990; Leary and Kowalski, 1990; Leary, 1996). A "significant portion of human behavior in organizations is motivated by impression management concerns, that is, by the desire to be perceived by others in certain ways" (Bozeman and Kacmar, 1997).

Goffman's (1959) seminal work on self presentation is generally considered as the cornerstone of modern research on impression management. Goffman only dealt with face-to-face interactions though, and did not directly discuss links between impression management and privacy. Later analysis in the domain of technology-mediated interaction interprets Goffman's work in the context of privacy and implicitly extends it to technology-mediated interactions (Ackerman and Cranor, 1999; Boyle and Greenberg, 2005; Lederer et al., 2003b; Palen and Dourish, 2003; Raento and Oulasvirta, 2008). Recent surveys on impression management research in the area of computer-mediated communication between people can be found in Albright (2001); Hancock

and Dunham (2001); Becker and Stamp (2001); Ellison et al. (2006).

Bozeman and Kacmar (1997) developed a self-regulation model of impression management processes in organizations. It describes an actor in a dyadic encounter who possesses a "reference goal" (the desired social identity that the individual wants to convey). The actor receives feedback from the "target" regarding the actually conveyed image, and continuously compares it with the reference goal. "If the comparisons indicate to the actor that the image he or she wants to portray is being achieved, then the tactics currently being used will be continued," and otherwise "if a discrepancy occurs, the actor will search for alternative tactics to use" (Bozeman and Kacmar, 1997). However, this model has to be enhanced in several respects for the purposes of IAIS and more specifically IM:

- IM users convey impressions to others not only during dyadic IM encounters, but at all times.
- The number of people to whom IM users convey impressions simultaneously (i.e., the number of people in their IM contact lists) is often considerably larger than in Bozeman and Kazmar's model.
- Targets can form impressions based not only on the current interaction and their recollection of prior interactions, but also on verbatim records of prior interactions that were archived as well as the awareness information that is conveyed through IM.
- IM users typically receive no feedback whether and when targets look at the abovementioned records and awareness information[1]
- The awareness information received by all targets is the same, even for those targets with whom one interacts rarely.

[1]See Hsieh et al. (2007) though for an enhanced system that provides some of this information.

- IM users can view the available awareness information indicators (e.g., the availability status indicators) to assess the conveyed impression, and can use system settings to disseminate information selectively in order to control this impression.

Based on the above discussion, we distinguished three separate types of impression in IAIS.

- The *intended impression* (also called *calculated* or *primary* impression (Schneider, 1981) or *desired image* (Leary, 1996)) is the impression that one aims to make on others.
- The *conveyed impression* is the impression that others actually form based on the awareness information that the system conveys about one, as well as the content of one's IM conversations with them (which others possibly archived). This conveyed impression is not directly observable by oneself.[2]
- The *predicted impression*, finally, is the impression that one perceives others will form owing to one's IM activity. The predicted impression is based on whatever information the system makes visible to oneself about one's IM activities, including the archived content of one's conversations if they were saved.[3]

### 6.1.5 Hypothesized Model

Since the conveyed impression is not directly observable, managing one's impression on others amounts to ensuring that the predicted impression is in line with the in-

[2]The possibility that different targets may form different impressions based on the same awareness information (Leary, 1996) is not directly relevant for the hypotheses of this research and will therefore be disregarded.

[3]Note that the predicted and the conveyed impressions may be formed on somewhat different grounds. For instance, one may be unaware that one's availability status has been "busy" for days (since one forgot to reset it), while this fact is clearly visible to others. Or one may not save conversations and thus forget about them, while others do so without one's knowledge and can resort to those even years later.

tended impression. A variety of cues have been found to be taken into account when gauging the impressions that are being formed, including feedback from others (Bozeman and Kacmar, 1997), publicly viewable information about oneself (such as ones profile and photo, Ellison et al., 2006), and system-conveyed awareness information such as the time one was last active (Ellison et al., 2006). Lee et al. (1997) report that users of their Portholes system (which takes snapshots of users every five minutes and disseminates them to collaborators to increase awareness) demanded that the system readily display several impression-relevant pieces of information, namely what images were taken of them, who can view their current image, and who selected to view their image at this moment.

We define the construct *visibility of one's conveyed impression to oneself* ("impression visibility") to denote the ready availability of cues for perceiving the impressions that are formed via IM. Based on the above research findings, we postulate the first hypothesis,

**H1: The desire to manage the impression conveyed to others affects one's desire for visibility (to oneself) of the conveyed impression.**

Moreover, as Kacmar et al. (1996) put it, "it is commonly accepted that individuals in organizations [...] control the information available to others about themselves in order to control the image presented." As discussed above, selective information disclosure was found to be the main tactic of IM users to attain the state of privacy that they desired (Patil and Kobsa, 2004, 2005a). In a cross-cultural study, Chen et al. (2008) also observed more specifically that "[a] person with an increased fear of negative evaluations [...] is more likely to exercise his/her privacy rights." This leads to our second hypothesis,

**H2: The desire to manage one's impression on others influences one's desire for privacy.**

Prior studies of computing systems pointed out that privacy desires are tied with the visibility of one's actions to oneself (Bellotti and Sellen, 1993; Bellotti, 1996), as well as the visibility of the actions of the system (in other words, the transparency of the system's operation) (Patil and Lai, 2005). Bellotti (1996) recounts a number of embarrassing incidents in which insufficient system feedback in media spaces had made users unaware that they were on camera, and suggests they would have behaved in a more privacy-conscious manner had better indicators been available. Lee et al. (1997) report that once users of their Portholes system could view the images that were taken of them and displayed to others, they were keen to delete unfavorable images or to show something else of their own choosing (they could not show different images to different people). This suggests that the desire for visibility (to oneself) of one's conveyed impression impacts one's desire for privacy with regard to others:

**H3: The desire for visibility (to oneself) of one's conveyed impression influences the desire for privacy.**

Taken together, these hypotheses postulate that the desire for privacy in IM is influenced by the desire to manage the impression that one conveys to others, and by the desire for having this impression clearly visible to oneself. This desire for visibility (to oneself) of the conveyed impression is also affected by the desire for impression management.

Figure 6.1 shows the three hypotheses in a causal factor structure.

## 6.2 Online Questionnaire

We sought to test and quantify the hypothesized relations presented Figure 6.1 through linear structural modeling of responses to an online questionnaire that was

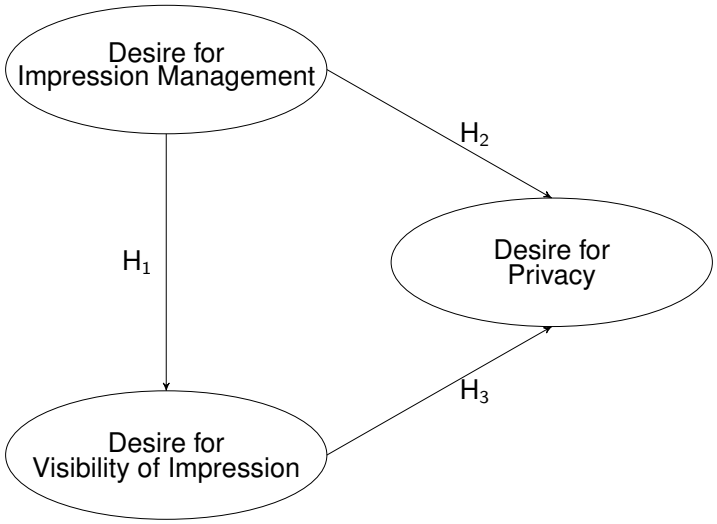


Figure 6.1: Hypothesized causal structure

developed based on the insights gained from the exploratory interviews.

### 6.2.1 Methodology

We developed a detailed online questionnaire aimed at understanding privacy attitudes and practices of adult (18 years or older) IM users (see Appendix A). Although our main interest was privacy, in order to avoid biasing responses as well as to frame privacy issues in the broader context of IM usage, the questionnaire also asked extensively about people's IM use in general.

One of the questions asked the respondents to rate how concerned they were about privacy when using IM. Separately, we asked them to rate their level of concern regarding others looking at their computer screen during IM conversations. For both of these questions, users entered a rating on a 7-point scale along with an open-ended explanation for the rating. Further, we asked respondents to rate their level of comfort with 10 pre-specified categories of people being able to access and read all of their IM conversations (past, present, and future). Users rated their comfort level on

a 7-point scale for the categories we provided: friends, family, colleagues, superiors, subordinates, classmates, significant others, ex-significant others, acquaintances, and strangers.

The questionnaire deliberately did not provide a definition of privacy since we were interested in understanding how users characterize the term instead of biasing them with a specific definition. We coded the open-ended user explanations for their level of privacy concern into a list of categories that we had developed based on the responses. Two researchers, with myself being one of them, acted as independent coders. Respondents often justified their ratings with multiple reasons. Such cases were classified into more than one category. Discrepancies in the coding were discussed and resolved until full inter-coder agreement was reached.

### Scales

In order to verify the above hypotheses presented in the previous section, we used questionnaire items to operationalize the three constructs: 'desire to manage one's conveyed impression' (*impression-mgmt*), 'desire for visibility (to oneself) of one's conveyed impression' (*visibility*), and 'desire for privacy' (*privacy*). The operationalization of all three concepts is based on our interviews with frequent users of IM (Patil and Kobsa, 2004, 2005a), on our analysis of privacy attitudes and practices in IM based on questionnaire responses (Patil and Kobsa, 2005b), and on findings in the literature regarding people's privacy-related behavior in computer-mediated interaction. Our final choice of items for the three concepts is explained below.

**Desire to manage the impression one conveys to others (impr-mgmt):**

Grinter and Palen (2002), and Patil and Kobsa (2004, 2005a) found that IM users – both teens and adults – managed their conveyed impression by

adjusting the various settings that IM systems make available for modification and customization (e.g., status messages). Thus, the following two items that deal with adjusting various IM settings are selected for the operationalization of the factor 'impression-mgmt':

a. Desire for the ability to specify IM software settings on a per individual basis

b. Desire for the ability to specify IM software settings on a per group basis

Respondents indicated on a 7-point scale how desirable they found adding the above features to IM. The items also tap into control over one's own availability, which was also rated as important by our interviewees (Patil and Kobsa, 2004, 2005a). In our sample of 622 survey participants (see below), internal consistency (Cronbach's alpha) of this scale was .80, $M = 3.90$, $SD = 1.66$.

**Desire for visibility to oneself of the impression conveyed to others (visibility):** The desire for visibility (to oneself) of one's impression was operationalized by the questionnaire items below. These items refer to features by which the IM system can increase the transparency of one's appearance to others:

a. Desire for the ability to see how I appear to my contacts

b. Desire for the ability to see how I compare with my contacts based on my settings, conversations, and history

c. Desire for the ability to see who has added me to their contact list

Again, for each of the above items, respondents indicated on a scale of 1-7 how desirable they found the addition of the particular feature to IM (Cronbach's alpha = .72, $M = 4.40$, $SD = 1.52$).

**Desire for privacy:** In our earlier work, the following aspects and antecedents of privacy desire were established as being most important for IM users:

a. Privacy from non-contacts (Patil and Kobsa, 2004, 2005a)

b. Privacy regarding the content of the IM communication (Patil and Kobsa, 2004, 2005a)

c. The sensitivity of the communication content (Patil and Kobsa, 2005b)

Our interviews had also indicated that these aspects manifest themselves in users' IM privacy practices in the form of selective information disclosure to their various IM contacts. Other studies, such as (Burgoon et al., 1989; Greene, 2000; Lederer et al., 2003b; Consolvo et al., 2005), had also found differences in privacy practices depending on the addressee. We therefore sought to capture these three aspects by the level of comfort respondents expressed with different groups of people being able to access and read all of their conversations (past, present or future). We chose eight common social groups that people use IM with: friends, family members, colleagues (peers), superiors, subordinates, classmates, significant others, ex-significant others. Another important determinant of privacy desires in IM is one's personal disposition towards privacy (Patil and Kobsa, 2005b), and we captured it by polling the privacy desires related to strangers.

The level of comfort with different groups of people being able to access and read all of the participants' conversations was elicited with a scale of 1-7 for each group. In our sample of 622 survey participants (see below), internal consistency (Cronbach's alpha) of this scale was .91, $M = 4.58$, $SD = 1.54$.

The assignment of questionnaire items to constructs is summarized in Table 6.1. The acceptable levels of internal consistency of each scale justify the assignment of items to their respective scale. The scales will also be tested for consistency with the help of confirmatory factor analysis and linear structural modeling (see the next section).

Table 6.1: Assignment of survey questions to constructs

| Question | | Abbreviation | Construct |
|---|---|---|---|
| Please indicate how important the addition of the following features to Instant Messaging is to you: | Ability to specify settings on a per individual basis | IMP1 | impr-mgmt |
| | Ability to specify settings on a per group basis | IMP2 | |
| | Ability to see how I appear to my contacts | VIS1 | visibility |
| | Ability to see how I compare with my contacts based on my settings, conversations, and history | VIS2 | |
| | Ability to see who has added you to their contact list | VIS3 | |
| Indicate your level of comfort with the following groups of people being able to access and read all of your conversations (past, present or future): | Friend | PRI1 | privacy |
| | Family member | PRI2 | |
| | Colleague (peer) | PRI3 | |
| | Superior | PRI4 | |
| | Subordinate | PRI5 | |
| | Classmate | PRI6 | |
| | Significant other | PRI7 | |
| | Ex-significant other | PRI8 | |
| | Stranger | PRI9 | |

**Sample**

An announcement of the questionnaire was distributed via various mailing lists, through personal contacts, and via postings to a large online community site (craigslist.org, subcategory *et cetera jobs*). We balanced our sample geographically by posting the announcement to more than a dozen metropolitan portals across the U.S. The first 40 respondents were offered a compensation of $5. We received 622 valid responses to the survey over a period of approximately three weeks. To avoid biasing the respondents, we did not reveal that the survey focused on privacy. Means,

Table 6.2: Means, standard deviations, and inter item correlations of measurement items ($N = 622$)

| | *M* | *SD* | (1) | (2) | (3) | (4) | (5) | (6) | (7) | (8) | (9) | (10) | (11) | (12) | (13) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1. MP1 | 4.24 | 1.81 | | | | | | | | | | | | | |
| 2. IMP2 | 3.55 | 1.83 | .66 | | | | | | | | | | | | |
| 3. VIS1 | 4.91 | 1.83 | .26 | .27 | | | | | | | | | | | |
| 4. VIS2 | 3.84 | 1.92 | .20 | .24 | .55 | | | | | | | | | | |
| 5. VIS3 | 4.43 | 1.94 | .18 | .20 | .44 | .41 | | | | | | | | | |
| 6. PRI1 | 3.21 | 2.01 | .05 | .08 | .06 | .02 | .16 | | | | | | | | |
| 7. PRI2 | 4.22 | 2.14 | .04 | .03 | .06 | -.02 | .10 | .65 | | | | | | | |
| 8. PRI3 | 4.76 | 1.91 | .08 | .06 | .08 | .04 | .15 | .61 | .66 | | | | | | |
| 9. PRI4 | 5.44 | 1.86 | .08 | .05 | .06 | .02 | .13 | .42 | .54 | .77 | | | | | |
| 10. PRI5 | 5.24 | 1.88 | .11 | .08 | .04 | .01 | .13 | .46 | .52 | .80 | .87 | | | | |
| 11. PRI6 | 4.63 | 2.04 | .14 | .09 | .09 | .05 | .12 | .52 | .47 | .70 | .68 | .75 | | | |
| 12. PRI7 | 3.43 | 2.21 | .03 | .04 | .03 | .07 | .12 | .64 | .57 | .53 | .44 | .47 | .48 | | |
| 13. PRI8 | 4.93 | 2.08 | .11 | .14 | .06 | .13 | .17 | .45 | .39 | .56 | .57 | .62 | .64 | .50 | |
| 14. PRI9 | 5.36 | 2.11 | .18 | .18 | .11 | .06 | .14 | .24 | .16 | .41 | .43 | .50 | .45 | .16 | .47 |

*Note.* All correlations $> .07$ are significant, $p < .05$.

Table 6.3: Means, standard deviations, and inter item correlations of measurement items ($N = 622$)

standard deviations, and inter-item correlations are presented in table 6.3.

### Factor Analysis and Linear Structural Modeling

**Factor Analysis** Prior to hypothesis testing, we verified the scales for the independent variable 'desire for impression management' and the dependent variables 'desire for visibility of impression' and 'desire for privacy' with a confirmatory factor analysis, conducted with LISREL 8.54 (Jöreskog and Sörbom, 2003). All measurement items of the privacy scale showed loadings of 0.85 or higher, all items of the visibility scale had loadings of 0.72 or above, and the two items of the impression scale exhibited loadings of 0.91 (IMP1) and 0.93 (IMP2). An RMSEA value of 0.063 indicates an acceptable fit of the solution. Our hypothesized scales are thus supported by the data. The average score across all participants for the Scale *Impression Management* was $M = 3.89$ ($SD = 1.54$), $M = 4.40$ ($SD = 1.52$) for *Visibility*, and $M = 3.89$ ($SD = 1.66$) for *Privacy*.

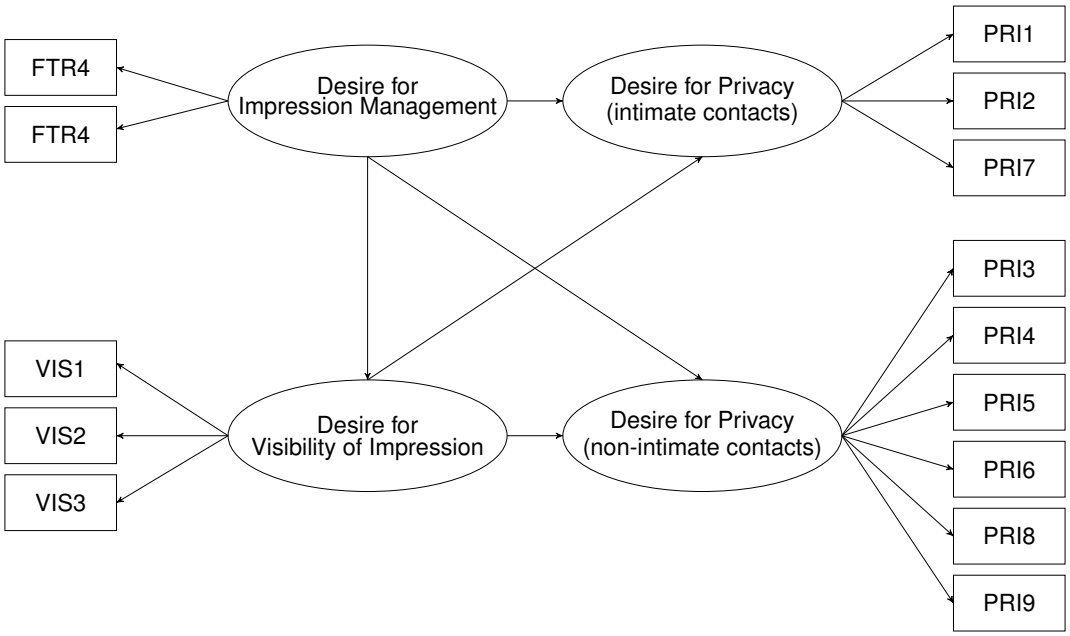


Figure 6.2: Alternative hypothetical model including different desires for privacy with regard to the intimacy of contacts

However, there is a strong indication in the literature that the relationship to the addressee has an effect on people's willingness to disclose certain information (Burgoon et al., 1989; Greene, 2000; Lederer et al., 2003b; Consolvo et al., 2005; Patil and Lai, 2005). Different levels of relationship to others could thus be a factor in people's desire for privacy. As the scale for desire for privacy includes different levels of relationship to others, we submitted the nine measurement items for desire for privacy to an explorative factor analysis with oblique rotation. The Eigenvalue >1 criterion revealed a two-factorial solution: the items 'friend,' 'family member,' and 'significant other' loaded on one factor (labeled as intimate contacts), the other items loaded on a second factor (labeled non-intimate contacts). Thus, an alternative hypothetical model is possible, in which our original privacy construct is replaced by two constructs: desire for privacy towards intimate contacts, and desire for privacy towards non-intimate contacts. This alternative model is summarized in Figure 6.2.

Table 6.4: Goodness-of-fit statistics for the original model and the alternative model

| Model | $\chi^2$ | *df* | *p* | GFI | CFI | PNFI | RMSEA | AIC |
|---|---|---|---|---|---|---|---|---|
| Original Model | 267.56 | 74 | $< .001$ | 0.99 | 0.98 | 0.70 | .065 | 329.56 |
| Alternative Model | 372.90 | 72 | $< .001$ | 0.98 | 0.98 | 0.77 | .082 | 483.90 |

**Linear Structural Modeling** We submitted both the original model (Figure 6.1) and the alternative model (Figure 6.2) to linear structural modeling. The constructs discussed in the previous subsection form the latent variables and the items used to operationalize the constructs form the corresponding indicators (effects). The directions of the arrows indicate the direction of causality. LISREL 8.54 (Jöreskog and Sörbom, 2003) and the SIMPLIS command language were employed to test the models on the questionnaire data. Since ordinal data was used, the weighted least squares algorithm for polychoric correlations was employed, including the asymptotic covariance matrices (Jöreskog and Sörbom, 1993).

### Results

The original structural model reached stable parameter estimates after fourteen iterations and is presented in Figure 6.3 (standard errors of measurement variables are omitted). All coefficients are statistically significant at the 5% level. In contrast, the alternative model did not reach stable parameter estimations below 1000 iterations. Manual specification of 10000 iteration led to stable parameter estimates. However, all of the standardized path coefficients between the latent variables (constructs) were larger than 1, reflecting the issues that LISREL encountered in its attempt to establish a fitting model.

Fit indices of both models are reported in Table 6.4. In order to evaluate and compare the model fit, we employed the criteria suggested by Schermelleh-Engel et al. (2003).

Although the Chi-square-to-degrees-of-freedom index (3.61) of the original model is out of the bound of the recommended $3 \times df$ threshold, the RMSEA value of .065 is still well below the .08 bound of acceptable fit. Furthermore, the fit indices Goodness of Fit Index (GFI) and the Comparative Fit Index (CFI) indicate a good fit, while the Parsimony Normed Fit Index (PNFI) indicates an acceptable fit. In summary, Chi-Square based measures of the original model indicate a poor fit, RMSEA-based measures indicate an acceptable fit, and the fit indices indicate an acceptable to good fit.

As regards the alternative model, seven out of the eight reported fit indices indicate a worse fit than for the original model (see Table 6.4). Combining this observation with the unstable parameter estimates, we deem the original model a better fit and reject the alternative model. The final original model with all relevant path coefficients is presented in Figure 6.3. The model accounts for 9% of the variance in desire for privacy[4] and for 26% of the variance in desire for visibility of impression.

The acceptable fit of the model permits us to now evaluate the assignment of measurement variables to constructs, and to test the hypotheses for causalities between the latent constructs. The former is supported by the measurement models (the coefficients between constructs and measurement variables), as all factor loadings between latent constructs and measurement variables are above 0.68. Moreover, all three postulated hypotheses are confirmed by the model, as is indicated by the positive significant path coefficients between constructs. Thus, the assumed factor structure (see Figure 6.3) can be found in the data.

[4]This low amount of explained variance should come as no surprise since privacy is contingent on many situational and individual factors (see Section 2.2.2). In the area of information privacy, for instance, more than a dozen determinants have been identified that affect people's stated or experimentally exhibited privacy concerns (see (Kobsa, 2007a,b) for a review).

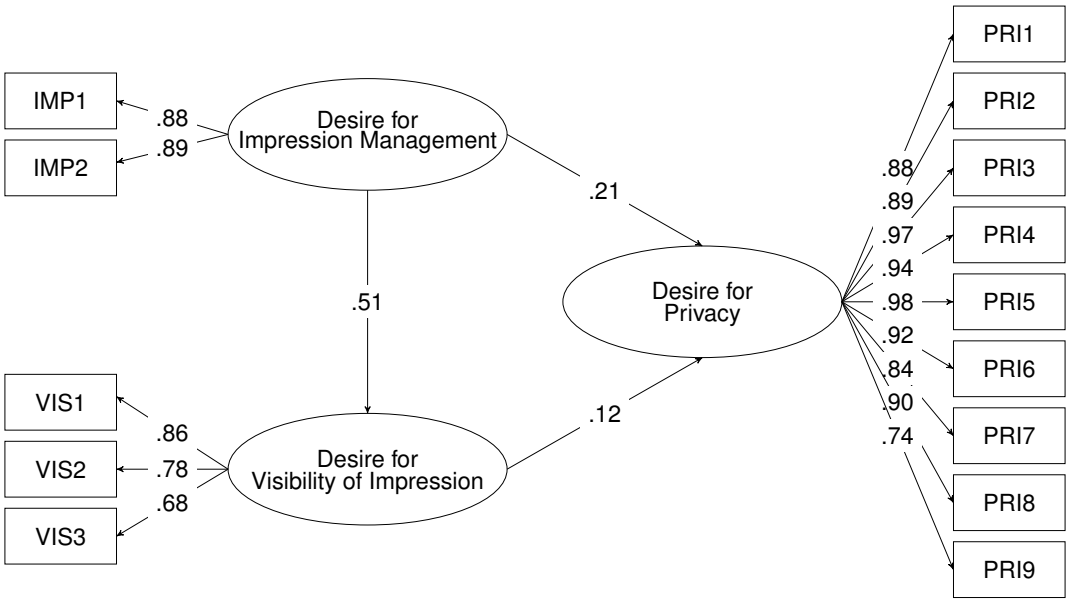


Figure 6.3: Path diagram of the linear structural equation model with path coefficients

### Unpacking Privacy Attitudes and Actions

User-reported concern about IM privacy (see Figure 6.4) spanned the whole scale from 1 (low) to 7 (high), and on average was slightly below "medium" (mean: 3.34, median: 3, mode: 4, SD: 1.7). Respondents' justifications for their rating of privacy concern revealed the following as the main contributing factors: sensitivity of content (33%), personal disposition towards privacy (25%), understanding of technology (22%), and potential persistence of conversations via archiving or logging (21%) . The relative frequencies of each of these four factors showed statistically significant correlations ($p < 0.05$) with the privacy concern rating.

Sensitivity of content relates to whether the respondent justified his or her rating for privacy concern based on the conversation as being either sensitive or not sensitive. Privacy concern was positively correlated with sensitivity ($p < 0.0001$ for not-sensitive and $p < 0.03$ for sensitive content, see Figure 6.5). Personal disposition towards privacy reflects a respondent's inherent attitudes. This encompassed comments in which

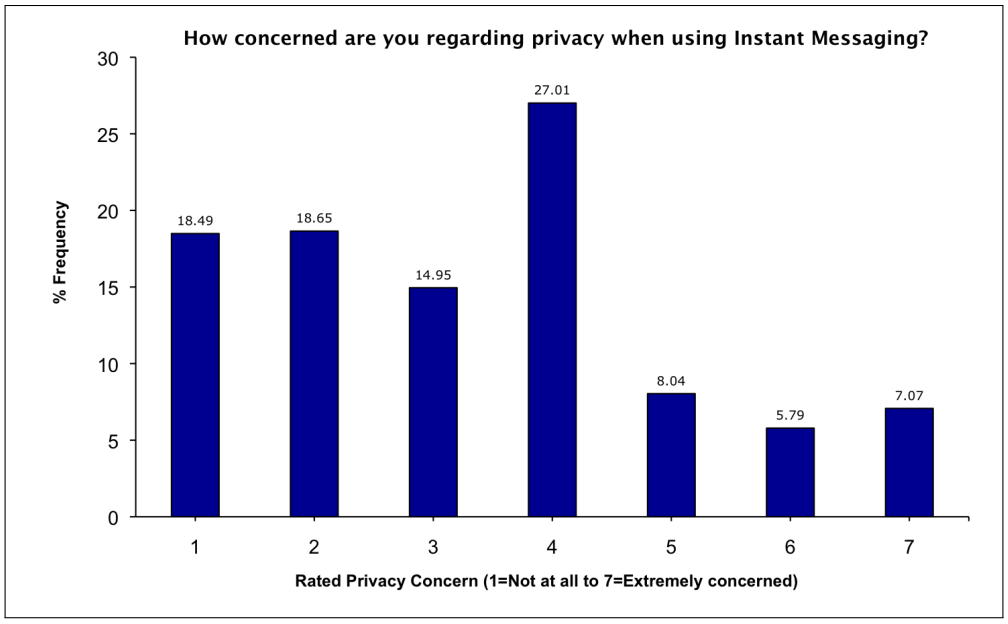


Figure 6.4: User-rated privacy concern on a 7-point scale

respondents expressed "indifference" ($p < 0.001$) as well as those in which respondents claimed to "value privacy" ($p < 0.1$). The frequencies of these justifications seemed to even be exponential rather than linear (see Figure 6.6). For instance, 85% of respondents who were "indifferent" toward privacy expressed privacy concern between levels 1 and 3 (and none as 6 or 7). On the other hand, 77% of those who said they "value privacy" were concerned about IM privacy between levels 5 and 7 (and none at 1-3).

Technology-based justifications were classified into three sub-categories: ignorance, misunderstanding and correct understanding. While "ignorance" was self-professed by the respondent, the classifications regarding accuracy of technological understanding were based on the judgment of the coders. Notably, we found a positive/negative correlation between understanding/ misunderstanding of technology, and rated privacy concern (see Figure 6.7). 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. For example, one

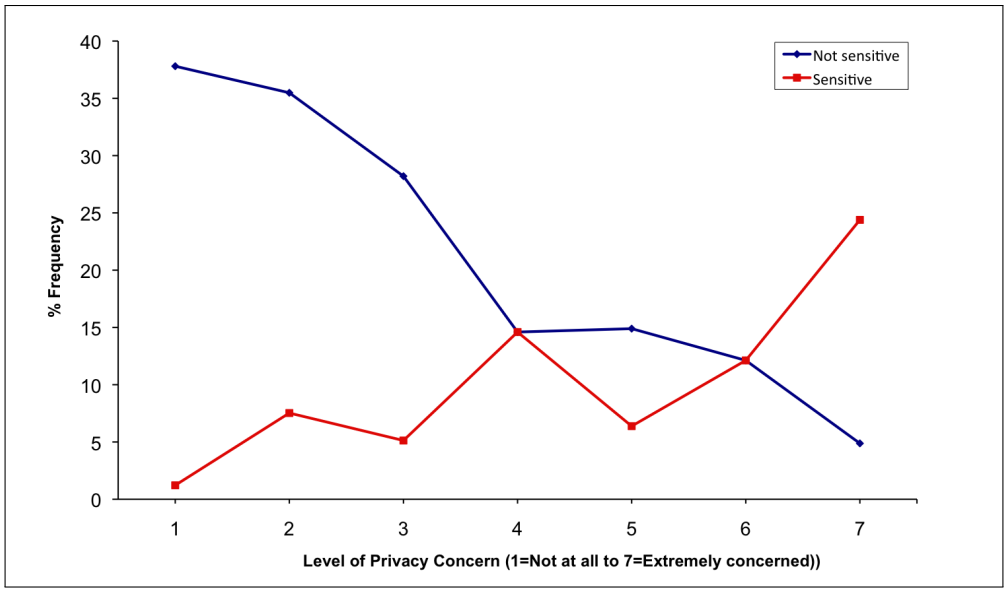


Figure 6.5: Impact of sensitivity of conversation

respondent with inaccurate understanding of the capabilities of a firewall rated his or her privacy concern as very low (1) while commenting,

> *"It's safe, right, if I have a firewall, and I'm talking to someone I trust."*

In contrast, another respondent who had an accurate understanding of technology was highly concerned (6) and remarked,

> *"All text is in the clear. Public IM services can store the text that I send, corporate (internal) services can do likewise and also monitor my availability."*

Self-proclaimed ignorance towards technology appeared to make users ambivalent (57% of those who said they were ignorant about technology indicated their level of privacy concern as 4, and 86% were between 3-5). This can be observed in Figure 6.7, where the line indicating "ignorance" peaks at the middle and falls away on both sides. This is also reflected in justifications such as,

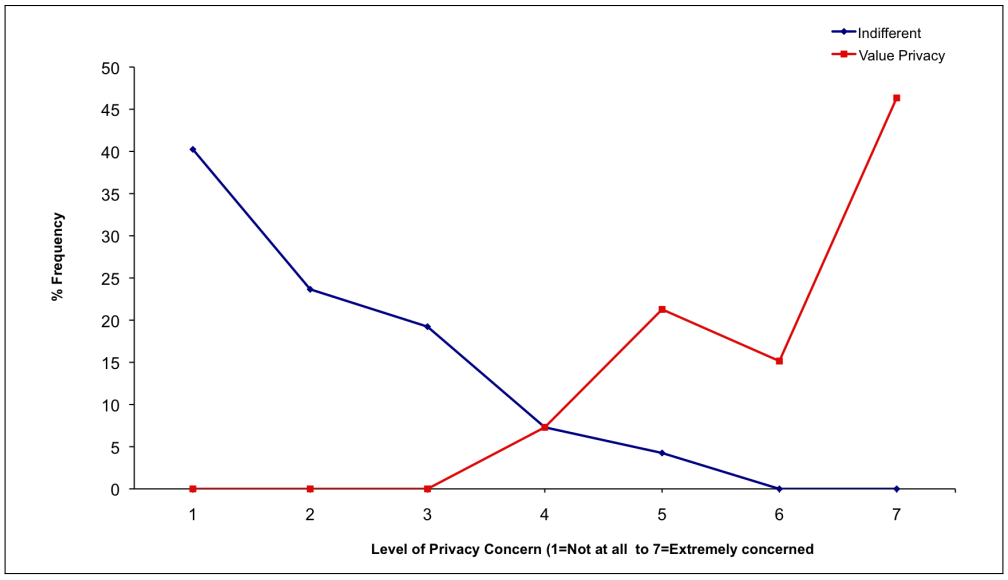


Figure 6.6: Impact of personal disposition towards privacy

*"It's not entirely clear to me how secure a conversation is on IM."*

Unsurprisingly, the degree of concern for others being able to view one's screen was positively correlated with the stated level of privacy concern ($p < 0.0001$). The mean (mean: 3.77, median: 4, mode: 4, SD: 1.8) was, in fact, slightly higher ($p < 0.0001$) than general concern for privacy. We suspect that this is due to the more tangible nature of the privacy threat experienced when someone can view one's computer screen. Again, sensitivity of conversation (43%) and personal disposition towards privacy (44%) emerged as two of the main factors (technological understanding and persistence were not applicable in this case). Compared to others, those who expressed higher personal desire for privacy were quite territorial about their computer screen while IMing ($p < 0.01$). They expressed that others looking at IM conversations "*feels like a violation of privacy.*" Location of IM use (25%) and relationship with concerned parties (20%) were also factors considered important by respondents .

The level of privacy concern correlated positively with respondents' degree of agreement regarding their IM behavior being altered by various factors (each $p < 0.01$).

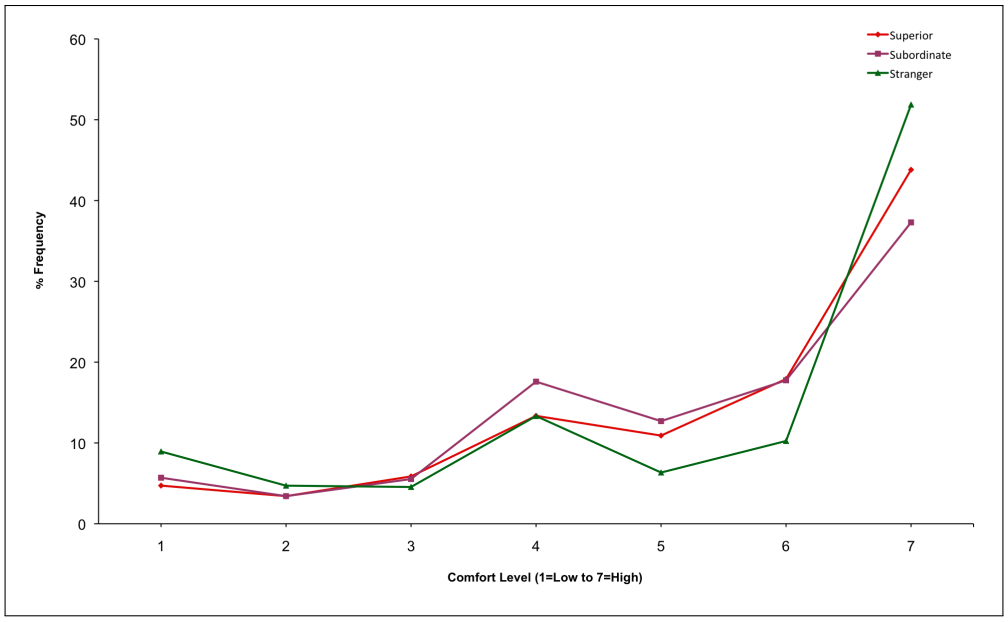


Figure 6.7: Impact of technological understanding

These factors included workplace policies, potential for sniffing of network traffic, or the ability for others to save conversations. That is, as can be expected, an increased concern for privacy is correlated with proclivity for "privacy-enhancing" actions and practices. Respondents who were more concerned with privacy were more likely to use encryption, to switch conversation medium for sensitive conversations, to lock their screens while away from the computer, and to change default settings of the IM system.

Finally, respondent expectations regarding privacy differed significantly for the various categories of contacts that we provided (paired t-tests for differences between most pairs of categories are statistically significant at $p < 0.0001$). In general, respondents felt more comfortable sharing their IM conversations with friends and significant others, than with any of the other groups. Interestingly, there was no statistically significant difference (paired t-tests), in terms of the level of comfort for sharing, between superiors and strangers, or between subordinates and strangers (see Figure 6.8). Given the high level of privacy one typically desires from strangers, this corroborates

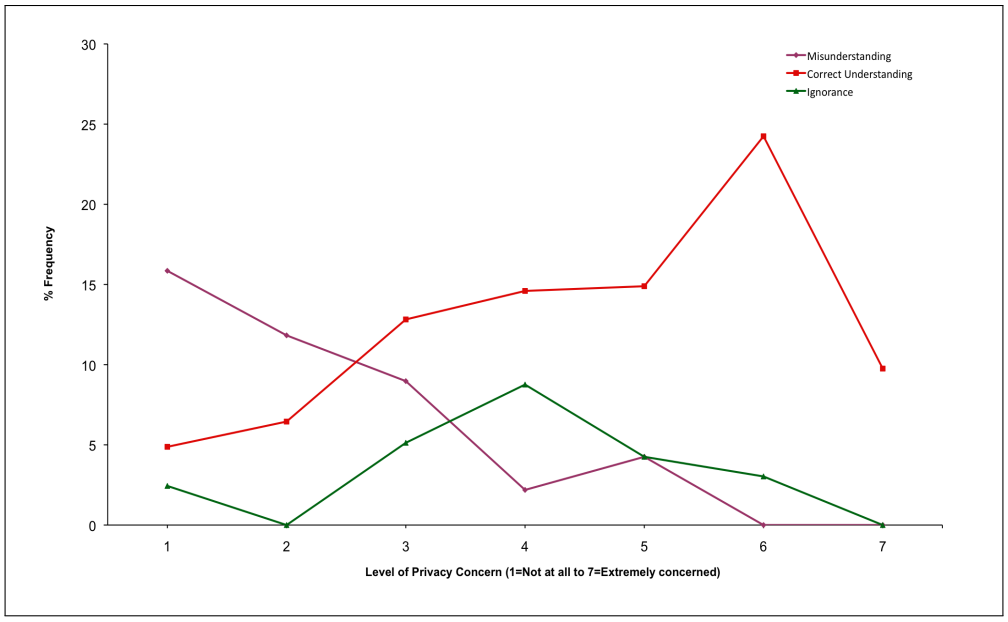


Figure 6.8: Privacy attitudes towards superiors, subordinates and strangers are similar

the finding of Lederer et al. (2003b) that hierarchical relationships may involve higher privacy tensions.

Our analyses indicated no significant effects of demographics except age (privacy concern increases with age, $p < 0.003$).

## Discussion

**Interpretation of the Results** Our model supports the existence of a causal relationship between one's desire for impression management and one's desire for privacy in the context of IM (H2). The two constructs are clearly distinct since the path coefficient of .21 is relatively small and since a coefficient of 1 is not included in the confidence interval. In addition, the model confirms that the desire for impression management also affects the desire for visibility of one's appearance to oneself, i.e., of the impression that IM conveys to one's contacts (H1). Being able to view these impressions on others in an effective manner would give one a better sense of the

adjustments that may need to be made (Leary, 1996; Bozeman and Kacmar, 1997). Further, our model also supports a causal relationship between the desire for visibility (to oneself) of one's appearance, and one's desire for privacy (H3).

Taken together, the model shows that the desire for privacy in the context of IM is not elemental and irreducible, but causally determined by impression-related factors. That is, IM users do not entertain privacy desires gratuitously but rather for at least one motive, namely their desire for impression management. The presence of impression management desire in the context of IM and its relationship with privacy desire is not accidental. For one, the desire for impression management is an omnipresent human social desire (see, e.g., Leary (1996): "virtually everyone is attentive to, if not explicitly concerned about how he or she is predicted and evaluated by other people"). On the other hand, selective information presentation happens to be a powerful tool for impression management. For instance, Leary (1996) found that "people manage their impressions not only by describing themselves in particular ways, but by excluding certain information from their self-descriptions." Goffman (1959) pointed out that self-presentation involves "the over-communication of some facts and the under-communication of others."

If the desire of IM users for impression management and selective information disclosure is to be taken seriously, then the design of such systems will need to cater to these desires. Based on the model presented in this paper, designers will need to improve the visibility of the impressions that IM users convey to others as a result of their IM activities, and to allow for a comparison of their activities with the prevailing practices of their IM contact groups. Users also need to be empowered to tailor these impressions differently for different contacts or groups of contacts, and may need continuous support in monitoring the actually conveyed impressions. We will therefore discuss design implications in the subsequent section.

**Limitations** Regarding possible limitations of this study, it should be noted that our results reflect privacy attitudes in the U.S. only. Given that traditions and opinions on privacy vary across cultures (INRA, 1997; IBM, 1999; Zhang et al., 2002; Ipsos Reid, 2006), the applicability of our results to a non-U.S. population would still need to be verified. While we aimed at a representative sample of adult IM users in the U.S., our sample consists mainly of urban and suburban residents; the rural population is underrepresented. Since the sample was mainly drawn from those who visit a specific online ad category, this may have introduced some additional bias. Finally, the sample has an inherent self-selection bias.

Eliciting all constructs with a single questionnaire at one point in time also gives rise to common method variance (Podsakoff et al., 2003) This might lead to inflated correlations that partially stem from statistical artifacts such as characteristics of the context in which the questionnaire was filled in by the participants, or characteristics of the items such as social preference identical format and identical response scale. Further research should thus aim at overcoming these issues by replicating our findings with different measures.

Regarding our linear structural model, it must be kept in mind that the correctness of such a model cannot be proven. A true model will indeed fit the data, but a model that fits the data does not necessarily need to be the true model. Given the grounding of our model development in prior literature as well as in the data,we believe that it represents the underlying data with reasonable accuracy. Yet, one cannot rule out that another model may fit the data equally well or even better.

Finally, our model only specifies a relationship between three different *desires* of IM users. It does not connect these desires with intended actions, such as adoption or usage of privacy-enhanced IM systems, let alone with actual behavior. The user evaluation in Patil and Kobsa (2010) goes one step further in this direction (see

Section 6.5).

## 6.3 Prototype Implementation of Enhanced IM Privacy Management

A general result of the analyses presented in Sections 6.1 and 6.2 is the insight that privacy research in the area of IM and, by extension, computer-mediated interaction in general, ought to include the notion of impression management since these two concepts are so tightly intertwined. Invoking Goffman who studied people-to-people interaction, Raento and Oulasvirta (2008) postulate that privacy and self-presentation need to be tackled together to also support computer-mediated human interaction. Our empirical findings support this conjecture. Consequently, privacy definitions in this area should particularly reflect the causal relationship between users' privacy desire and their desire for impression management to influence the evaluation by others.[5]

### 6.3.1 Design Implications

We believe that our model has four main implications on the design of IM systems that can take users' privacy and impression management desires far better into account than is presently the case. We list them below roughly in the order of increased expected benefit for users, which however correlates with increased implementation efforts.

[5]One of the rare examples of such a privacy definition is from Johnson (1989); Introna (1997); Introna and Pouloudi (1999), who characterize privacy as immunity from the judgment of others.

### Better Visibility of One's Actions to Oneself

As discussed before, the clarity with which one is able to view one's conveyed impression strongly affects the extent to which one's predicted impression is likely to correspond to the actually conveyed impression. This visibility can be improved in part by more effective system feedback that highlights the effects of one's actions to oneself (Bellotti and Sellen, 1993). For example, users' predicted impression about changes in their IM status (e.g., "busy," "idle," "using application x") will correspond much better to the actually conveyed impression if the status is not only conveyed to others in the form of awareness information, but also made visible to the users themselves.

Another form of visibility that improves users' perception of impression is the availability of indicators that allow them to evaluate how others perceive them. As Table 6.1 shows, one of the items for impression visibility (to oneself) is the desire to see how one appears to one's contacts. Begole et al. (2002) logged and mined interactions, with the IM system itself (e.g., login, logoff, status change) and with one's IM contacts (e.g., conversation lengths and times). While the authors used such logs to detect rhythms and make predictions, this information could also be made available to the users themselves in an interactive format. Users may then be able to derive a better sense of their own IM activity over time. For instance, they can find out how frequently others see them as "busy," or how quickly they reply to initial IM requests (e.g., from specific contacts like their senior co-workers or in general (Avrahami et al., 2008)). Such information may be useful in judging the impression that one conveys to others through one's IM activity. Without system support, such information is derived mainly from one's recollection of one's IM activities, which may be incomplete, incorrect, and possibly biased by one's self-image. System support for reflecting on one's activity in an interactive manner not only provides more objective information

but also lessens the cognitive burden of remembering it.

Finally, the visibility of one's actions to oneself can be improved through technical transparency. In the questionnaire responses, we found that those who understood the underlying technology better were also able to evaluate the privacy risks associated with their actions more correctly (Patil and Kobsa, 2005b). For instance, respondents with higher technical competency understood that unencrypted IM conversations could be captured by anyone on the network. Such an understanding, in turn, affected changes in the content and manner of the conversations. Higher system transparency facilitates users' understanding of how their actions are translated by the system, what effects the actions will produce, and what impressions they may convey.

### Better Visibility of Collective Practices

Impression visibility also involves the desire of users to compare themselves against prevailing collective practices (see Table 6.1). However, collective practices are often opaque and typically not articulated. This is especially true for relatively new and constantly evolving collaboration tools like IM. Insufficient knowledge of the prevailing practices in one's groups can make impression management challenging since it is difficult to form predicted impressions in the absence of a point of comparison. Indeed, Festinger's (1950; 1954) social comparison theory postulates that people desire to compare themselves with others.

To increase the visibility of one's impression to oneself, functionality should therefore be provided that aids in the discovery of collective practices, along with appropriate mechanisms for comparing one's own practices against them. For example, an IM system could provide a breakdown of the time various contact groups stay in different IM statuses on average (e.g., "while being logged in, contact group members were

available 45% of the time, away 15% of the time, and at lunch 5% of the time"). Such group information would provide a benchmark against which one could compare one's own practices, and would help gauge the impression one conveys in relation to the collective. The groups for whom collective practices are disclosed could be pre-defined (e.g., all employees of the company), or user-defined (e.g., one's project members). However, care must be taken that the group size remains large enough to avert the inference of information about individuals from collective data.

**Fine-grained Controls for Impression Management**

Traditionally, IM systems have relied on global preference settings for all of one's contacts. However, our interviews and questionnaires indicate that users desire the ability to configure settings differently for different contacts and groups of contacts (Patil and Kobsa, 2005b). We therefore recommend providing support for the adjustment of all impression-relevant settings at a finer grain (by "impression-relevant" settings we mean all whose effects are conveyed to others). For instance, IM users may choose to let only certain contacts see how long they have been idle, or not allow certain groups of contacts save their mutual IM conversations. Our interviewees even expressed a desire to use different conversation fonts and display pictures ("buddy icons") for different contact groups (e.g., professional ones for interacting with colleagues, and funny or cool ones for friends and family). Such fine-grained controls will aid IM users in conveying different impressions of themselves to different contacts and contact groups.

It is heartening that the newest versions of a few IM programs have included group-level adjustments for a small number of settings (notably one's IM status). We suggest that this be extended to all impression-relevant settings. Since the explicit specification of such impression management preferences for different groups of contacts is

cumbersome, it should be supported by suitable defaults whose appropriateness for each contact group could be determined empirically. For instance, Patil and Kobsa (2005b) found that superiors and subordinates are the least trusted categories of contacts. Consequently, the disclosure defaults for those two groups should be the most restrictive. Given the general proclivity of users to not change defaults, it may be worthwhile to make the installation of IM more interactive, in order to allow users to adjust those defaults during this process. Moreover, preferences that are in effect during an ongoing IM communication should be made visible and easily changeable *in situ* if such a need arises.

### Seeing the Actually Conveyed Impression

The Faces system (Lederer et al., 2003b) allowed users to specify how accurately personal information should be disclosed to a specific inquirer in a specific situation (namely "precisely," "vaguely," or "not disclosed"), and thereby to control their privacy on a per-person and per-situation basis (which would be a fine-grain control for intended impression in our terminology). In an evaluation of Faces, participants first specified disclosure preferences for a number of situations. After a pause of five minutes, they were presented with the same situations, and asked about their perceptions (predicted impressions) of what information was being conveyed (conveyed impression). Even though the time difference was very short and subjects had configured the conveyed impressions themselves, significant mismatches were observed between the currently predicted impression and the intended impression since users had seemingly forgotten some of their settings.

This experiment serves as a warning that it may not suffice to give users fine-grained control over their conveyed impression. Rather, they will also need a constant reminder of their intended impression. Also from a more practical perspective, users'

settings for fonts, colors, display image, etc. may be overridden by their contacts. Moreover, contacts may not be able to view the intended emoticons or hear the intended sounds due to differences in the IM clients at each end. Such mismatches may cause some loss in the originally intended impression that is not visible to the user. Being able to look at oneself from someone else's perspective could help mitigate disparities between the intended and the conveyed impression.[6] Users may possibly even want that certain awareness information be permanently displayed in their own IM clients in exactly the same form in which it can be viewed by certain important contacts, as a constant reminder of the impression that their IM system conveys to these select contacts.

## 6.4 PRISM: PRIvacy-Sensitive Messaging

Findings from the interviews and survey indicated 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.

[6]Raento and Oulasvirta's (2008)) smartphone-based ContextContacts system makes it possible to view oneself from the perspective of others, but the system conveys the same awareness information to everyone and is restricted to location and activity information. The authors envisage the implementation of group-specific disclosure and self-views though.

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., 2003b). 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.

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, to set expiration dates for saved conversations, to compare themselves with their contacts, and to know how they appear to their contacts via IM.

To overcome these limitations and shortcomings of current IM systems uncovered by our empirical findings, we designed PRISM (PRIvacy-Sensitive Messaging), which incorporates some of the above design implications (Patil and Kobsa, 2010). To en-

hance the support for privacy management in IM, PRISM provides solutions that address the aspects discussed above, viz., archiving of conversations, visibility of the actions of others and oneself, and differing attitudes toward different groups of contacts. In particular, PRISM provides IM users with various visualizations that allow for greater visibility (to oneself) of one's own actions in relation to one's contacts (e.g., temporal patterns of login activity, periods of idleness). The visualizations also facilitate the comparison of one's behavior with the collective activity of a contact group, such as one's colleagues or subordinates. Furthermore, PRISM provides mechanisms for presenting oneself differently to various groups of contacts by selecting different impression-relevant settings for them.

In designing PRISM, we also 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.

**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 a plugin for 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

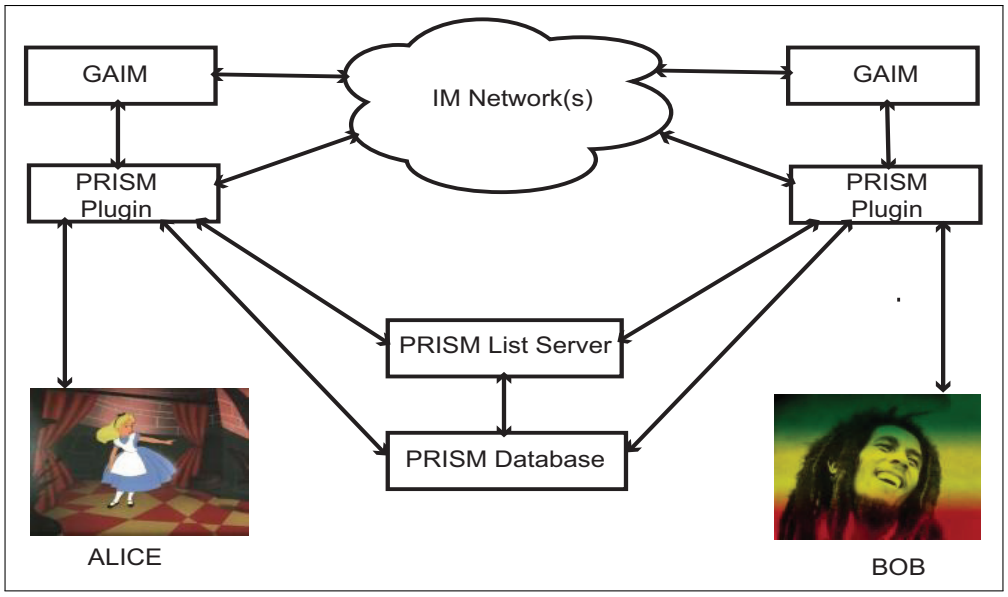


Figure 6.9: System architecture of PRISM

ability to access most popular IM networks such as MSN®, Yahoo!®, AOL®, and ICQ®. In the following subsections, we first describe the architecture of PRISM, and then present the specifics of our design in terms of the functionalities provided.

### 6.4.1 System Description

PRISM's extensions to the standard GAIM functionality are packaged as a plugin. The architecture of the system is shown in Figure 6.9. 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 6.4.2).

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.

### 6.4.2 Functionalities

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

#### 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.

### 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 6.4.3).

### 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, copy/paste text, and capture and 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 6.4.4).

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[7]. Prior to expiration, PRISM also allows the parties to renegotiate the expiration date should this be deemed necessary.

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

### 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 is 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.

### 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 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

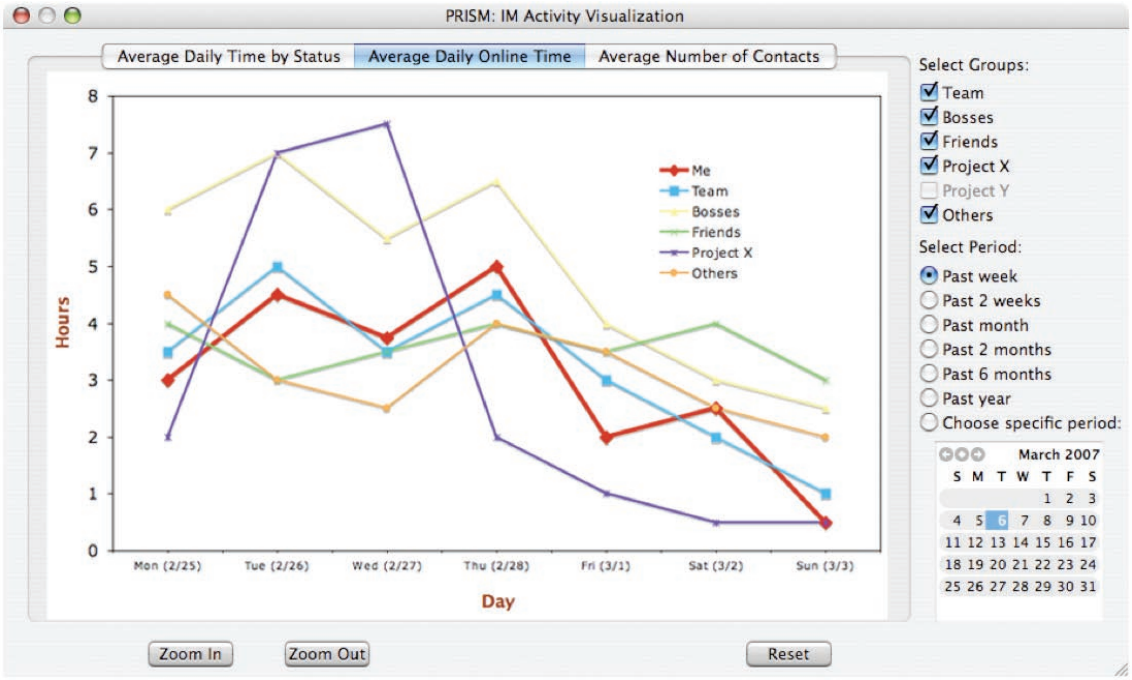


Figure 6.10: Visualization of average daily online time by contact group

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.

### 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 (Patil and Kobsa, 2005a; Kobsa et al., 2010). 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 con-

veyed 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 6.10 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 6.10, 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 for 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 6.10, 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 valuation 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 6.10), IM status when online, and average number of IM contacts. We chose these particular activities because our interview subjects indicated that the 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 conversations (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.

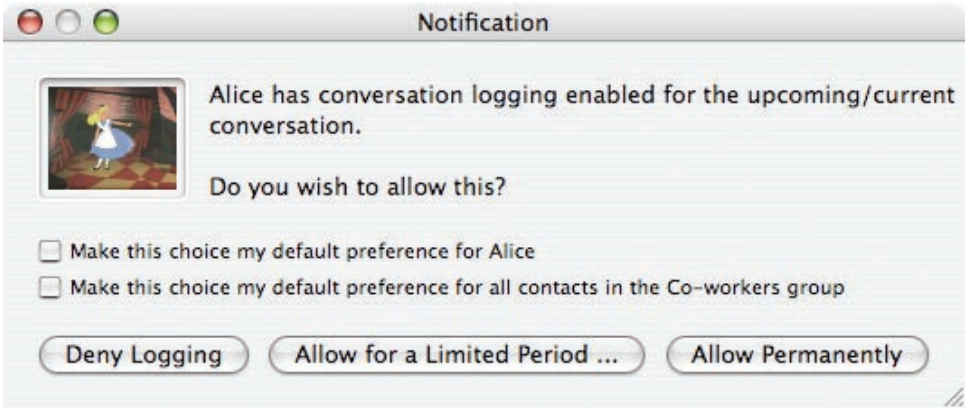


Figure 6.11: Notification of preference mismatch

**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.

### 6.4.3 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 6.4, 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 from their boss on a report. She notices in her IM contact list that Bob is online, and

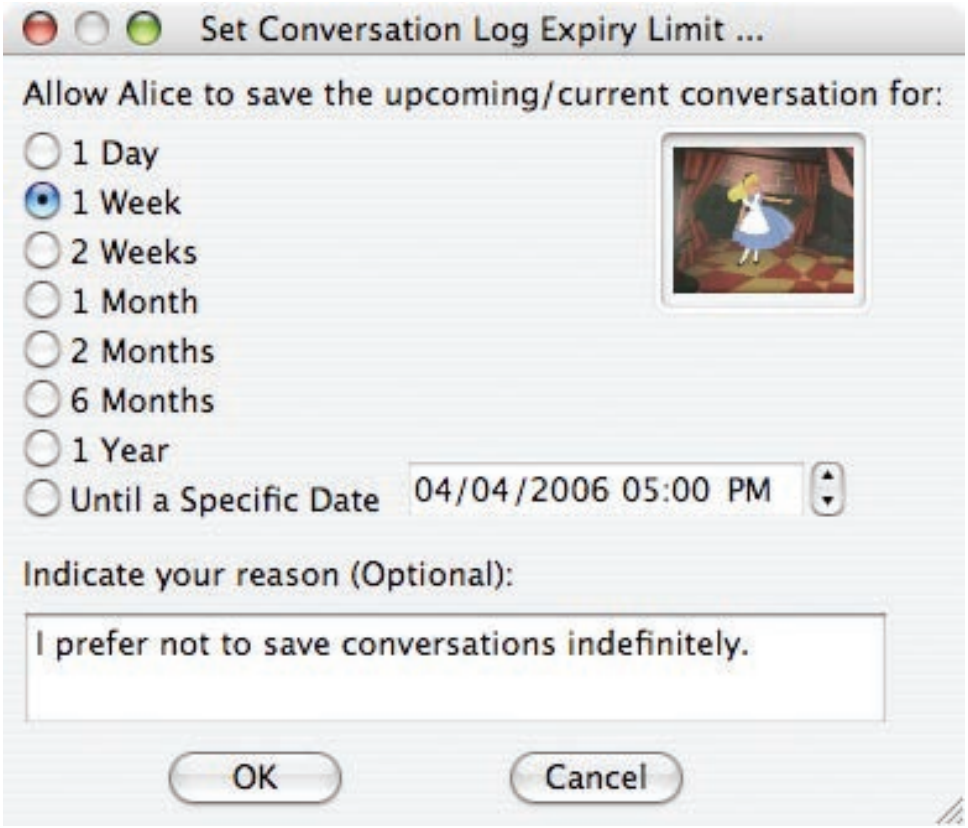


Figure 6.12: Setting expiry limit for conversation log

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 6.11). 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.


Figure 6.13: The choice made by the remote user

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 6.12). Alice is informed accordingly (see Figure 6.13). 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 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 6.11).

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*).

### 6.4.4 Discussion

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. 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.

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.

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.

**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 6.11).

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. (2003c) 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.

### 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.

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.

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).

## 6.5 User Evaluation of PRISM

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.

### 6.5.1 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 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.

### 6.5.2 Results

The results indicate that users believe that PRISM offers improved IM privacy management. Figure 6.14 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 conversations & 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 loosely coupled collaborative work.

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

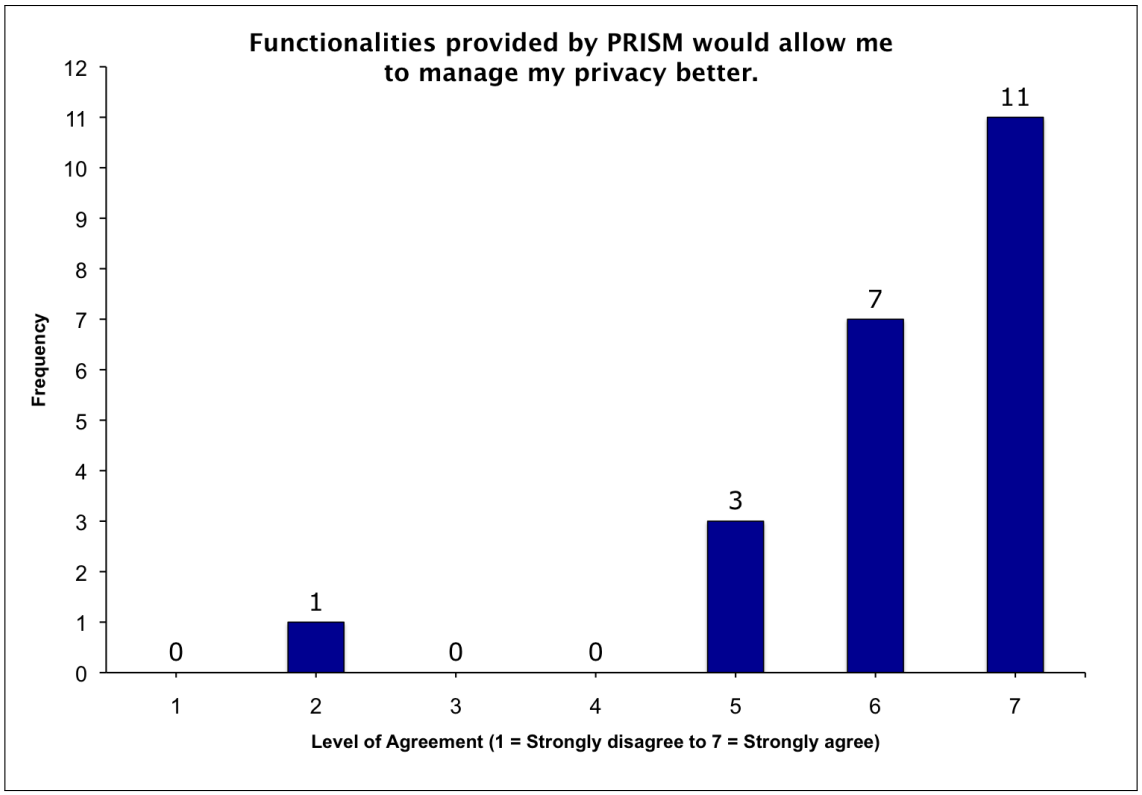


Figure 6.14: Users indicate that PRISM improves IM privacy

usage (see Figure 6.15). 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" sub-score (each $r \geq 0.58$, $p < 0.01$). Similarly, the utility of features of PRISM that pertain to control over conversation archives (viz., conversation expiry, encrypted archives,

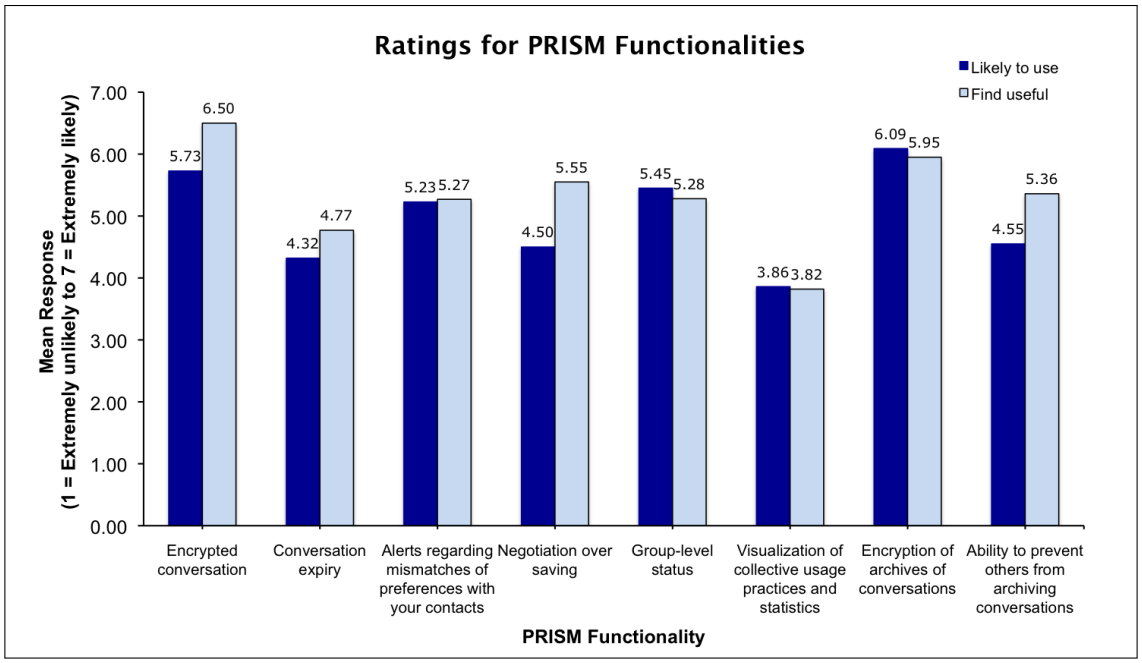


Figure 6.15: Utility and likely use of PRISM functionalities

and the ability to prevent others from saving conversations) showed statistically significant correlations with the "Unauthorized Secondary Use" subscore of the Smith et al. (1996) scale (each $r \geq 0.41$, $p < 0.05$). Both of these subscores also correlate significantly with the utility of the group-level preference specification feature (each $r \geq 0.41$, $p < 0.05$). 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 6.15. 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 and 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.

### 6.5.3 Insights for Usability Evaluation of Privacy Designs

While 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. Unfortunately, our attempt in deploying PRISM did not succeed. As the following discussion will show, the failure was unrelated to the functionalities of PRISM. Although we failed in our attempt to achieve a more extensive and contextual user evaluation, the failure provided numerous insights regarding conducting usability studies of privacy aspects of IAIS. We believe that the lessons we learned are useful for those who wish to design and conduct such studies in the

future.

### Description of the Study

We attempted a longitudinal user study to evaluate the extent to which PRISM met its objective of improving IM privacy management. The study involved a quarter-long, upper-division undergraduate course at a large public university in the U.S. The course required the students to engage in a team project that lasted through the quarter. Each team comprised 4-5 students. The teams worked on projects defined and managed by external "customers" who came from both within as well as outside the university. The subjects of the study were the students, the customers, the instructor, and the teaching assistant.

The first two weeks of the quarter were utilized for instructions and setup. After filling out a pre-study questionnaire, all subjects were required to install GAIM. They were also asked to create a separate IM account for class purposes. The students were asked to add their project partners, the instructors and their customers to this account and vice versa. Additionally, 5 out of the 9 project teams and their customers were asked to install PRISM. The other 4 teams and their customers were assigned to the control group. The teams that installed PRISM were asked not to divulge the installation of the plugin to those in the control groups. We used a short verification questionnaire to ensure that all subjects had installed GAIM and/or PRISM successfully, and that they were aware of its functionality. However, in order to avoid biasing the participants we took care not to make references to privacy in any of the questionnaires.

Subjects were then asked to use the class IM account throughout eight weeks of the rest of the quarter for the purposes of collaborating with their project partners, customers, instructors and other classmates. During this period, a server collected

logs of user interactions with PRISM. To account for the time required for learning how to use GAIM and PRISM, we discarded the first two weeks of logs. At the end of the quarter, subjects filled out a post-study questionnaire, which asked them in detail about their experiences with PRISM.

### Lessons Learned

To our surprise and disappointment, we were unable to achieve sufficient usage to be able to evaluate the privacy mechanisms provided by PRISM. Upon reflecting on the reasons for the lack of usage, we believe that the following important lessons can be learned (Patil and Kobsa, 2009). It should be noted that these lessons need to be considered *collectively* and *simultaneously*; addressing only some of the lessons will not be adequate.

1. **Class project collaboration falls short of simulating collaboration in a knowledge-work organization.** A major motivation behind our IM studies was to explore the utility of IM as a means for collaboration and communication in knowledge-work. As a result, many of our design ideas were targeted at users engaged in collaborative knowledge work across multiple work spheres (González and Mark, 2004). We expected that a course with a collaborative project, which required interactions with one's team members, other classmates, instructors, and customers, would be sufficient as an approximation of a collaborative knowledge-work environment. However, we discovered that the amount of shared context and simultaneous online time among students taking the same course is far lower than among knowledge workers collaborating on a project. As a result, we discovered that most collaborative activities of the students took place either during scheduled face-to-face meetings or completely

asynchronously via email. Knowledge workers, in contrast, spend a large portion of their work time online in front of a computer with significant overlaps in their work hours. This fact, coupled with the shared context of the organizational affiliation, creates much greater incentives and opportunities for IM usage.

There are at least three major domains in which systems for interpersonal interaction are used: professional, social and educational. Our experience suggests that careful attention must be paid to the similarities and differences between these domains as well as the rigidity (or fluidity) of the boundaries placed by an individual when moving between them.

2. **Undergraduates are not representative users.** Ideally, it is desirable to conduct a user study on a sample of the target population. Often times though, access to the target population is prohibitively difficult. The ease of access to undergraduate students makes them an attractive population for conducting user studies.. However, the use of undergraduate populations in a study could jeopardize its external validity. For privacy studies, this sampling bias has an even greater impact because undergraduates are known to have different privacy attitudes and behaviors than older adults (Dommeyer and Gross, 2003; Milne and Boza, 1999; Patil and Kobsa, 2004). Moreover, a person's age is known to have an effect on privacy concerns (Campbell, 1997). In order to mitigate the impact of these factors we utilized an upper-division course with older undergraduates, and provided the context of collaborative team projects. Unfortunately, we found that a course that meets only three hours each week is not enough to transcend the impacts of age and of the "undergraduate lifestyle" (for instance, undergraduates take several classes, work part-time jobs, and are often mobile across campus locations). A possible compromise is to utilize graduate students, faculty, and staff as subjects.

3. **A longitudinal study does not guarantee the usage of privacy management mechanisms.** Typically, a longitudinal study is necessary for an effective evaluation of privacy management designs. However, we found that running a study over a long period of time may not be *sufficient* for ensuring that the privacy management mechanisms are used by the subjects. This situation arises because privacy management is a secondary function in the overall system usage. A user's desire and attention are focused on the primary function of interpersonal interaction; privacy management comes into play only when required. As a result, privacy management functionality forms a very small portion of the overall system usage to begin with. Infrequent use also leads to a vicious cycle where users do not utilize the privacy management functionality, even when desired, because they forgot about its existence and/or because they are less familiar with its operation, owing to the lack of sufficient use. Further, some users may never engage in additional privacy management if the default system behavior and preferences satisfy their privacy needs adequately.

   These observations suggest that the length of such studies needs to be longer than that for a typical longitudinal user study. The study could also introduce external stimuli that require the user to use one or more of the privacy management mechanisms. Study confederates who deliberately engage in privacy-insensitive behavior is an example of such a stimulus.

4. **Prototypes cannot overcome switching costs.** PRISM worked only with GAIM[8]. To ensure that students would use GAIM instead of the IM client they normally used, we required the creation of a separate ID, and mandated that only this ID be used for all matters related to the class. Although responses to the post-study questionnaire reported an occasional lapse, our subjects did

[8]GAIM was chosen because – unlike the other commercially developed, IM-system-specific clients – it is open source, cross-platform, plugin-based.

comply with this policy overall. We did not prohibit the use of GAIM and PRISM for non-class IM activities. Yet, for all other (i.e., non-class) IMing purposes (which represent the vast majority of their IM activities), the subjects switched to their regular IM program. The enhancements of the plugin, which targeted the secondary function of privacy management, did not provide sufficient incentive to switch from other programs that provided a more familiar, convenient and polished user experience for the primary IM functions. Additionally, unlike the other IM programs, GAIM and PRISM were not available on the lab computers which are used frequently by undergraduate students.

This lesson regarding the costs of switching from the user's primary system is not limited to IM. For example, if privacy management functionality for a Web browser is packaged as a plugin available only for the Internet Explorer browser, users of other Web browsers, as well as other operating systems besides Microsoft Windows, will most likely choose to forgo the secondary enhancements than incur heavy switching costs for the primary activity of browsing the Web. An ideal solution to this problem is to develop the privacy plugin for all possible browsers on all possible platforms – a task that is daunting, if not infeasible. A more modest alternative is to develop privacy mechanisms in various domains of interpersonal interaction systems (e.g., IM, social networking, etc.) as cross-platform open standards similar to P3P (http://www.w3.org/P3P). Having such standards enables implementation by a wider community of institutional or individual software developers.

5. **Meaningful evaluation requires involvement of the entire set of contacts.** As mentioned earlier, systems for interpersonal interaction involve entire sets of people who are interconnected in the form of a social network. By studying one such network, viz. the students, instructors and customers of the project course, we believed that we would overcome the limitation of single-

user usability studies that do not take into account parties besides the user himself or herself. However, in the case of privacy, it turned out that investigating a small sub-network did not suffice; the entire network of IM users needed to be included. As mentioned earlier, privacy management practices typically require adoption over time and/or co-evolution, either of which is unlikely to occur within a sub-network of users, especially one much smaller than the larger network that has no access to the privacy management enhancements.

Consider, for example, a situation in which privacy management functionality in the context of mobile phones was available only to the users of a specific handset. Splitting one's communication network between those who posses the handset and those who do not would undermine the collective evolution of the shared experience surrounding privacy management mechanisms, hampering the attempts at evaluating their effectiveness. Access to entire networks of users is possible only with cooperation from the owners and administrators (organizations or individuals) of the specific systems. Achieving such cooperation requires actively pursuing collaborative ventures with industry partners.

6. **Defining what constitutes success is complicated.** We asked subjects to rate the utility of the different pieces of privacy management functionality added by our plugin, as well as their likelihood of adopting these enhancements. We expected that higher averages would be a measure of success for a given functionality. However, subject responses indicate that users have opposing opinions regarding some of the enhancements. For example, some subjects found a given feature to be great value, while another one was indicated to be not so useful. Another set of subjects, however, expressed nearly opposite opinions regarding the same two features. In retrospect, it seems natural that opinions regarding a nuanced, personal, and context-dependent concept such as privacy could evoke opposite opinions. Secondly, it is quite likely that different

users would find differential value in different privacy management features.

This situation makes it difficult to decide which metrics should be used to measure the "success" of privacy management designs. Should success be gauged for each feature separately or as an entire "privacy management user experience"? How does one isolate the impact of each piece of functionality on the overall experience of privacy management? An additional factor to consider is the mismatch between the stated opinions of the users and their captured actions, as reflected in the usage logs and observations of interaction (Berendt et al., 2005). How should these mismatches be reconciled for measuring success? Moreover, to account for learning and the evolution of practices, it is also important to measure the relevant metrics at multiple points in time during the study.

## 6.6 Conclusion

Our extensive investigation of privacy in IM usage uncovered important insights regarding privacy attitudes and behaviors that are important for reconciling privacy and awareness needs. We were also able to tackle our hypothesis regarding the role of impression management (see Chapter 3) in such reconciliation. The linear structural model that we postulated, and then verified empirically, shows that Goffman's finding on impression management can be extended to the digital domain with the additional consideration for the visibility of the impression(s). Based on the findings and insights from the studies, we designed solutions for enhancing IM privacy and built a prototype that demonstrates them practically. User evaluation of the prototype confirms its utility for improving current IM privacy management. At the same time, the evaluation efforts yielded several lessons that will be useful for future usability studies of privacy designs.

These results also set the platform for extension to other IAIS utilized in loosely coupled collaborations. As the following two chapters will show, we were able to confirm the applicability of these findings beyond IM.

# Chapter 7

# MySpace: Awareness Application for the Workplace

To include other systems in addition to IM, we studied an awareness application designed for the workplace. 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. The goal of mySpace is to support the communication and collaboration needs of workers. This includes locally mobile workers, workers who travel to the different buildings where a corporation does business, and those who telecommute. With its explicit focus on fostering awareness for loosely coupled activities among colleagues who share a common organizational bond, mySpace can also be considered to lie in the shaded area in Figure 4.2. Like other applications of this type, it inherently raises issues of privacy. To understand how users reconcile privacy and awareness needs at the workplace, we examined they defined privacy permissions in mySpace. The goal of the study was also to take a first step towards understanding the type of default permissions that would allow users to operate comfortably with the level of context sharing that is available through awareness

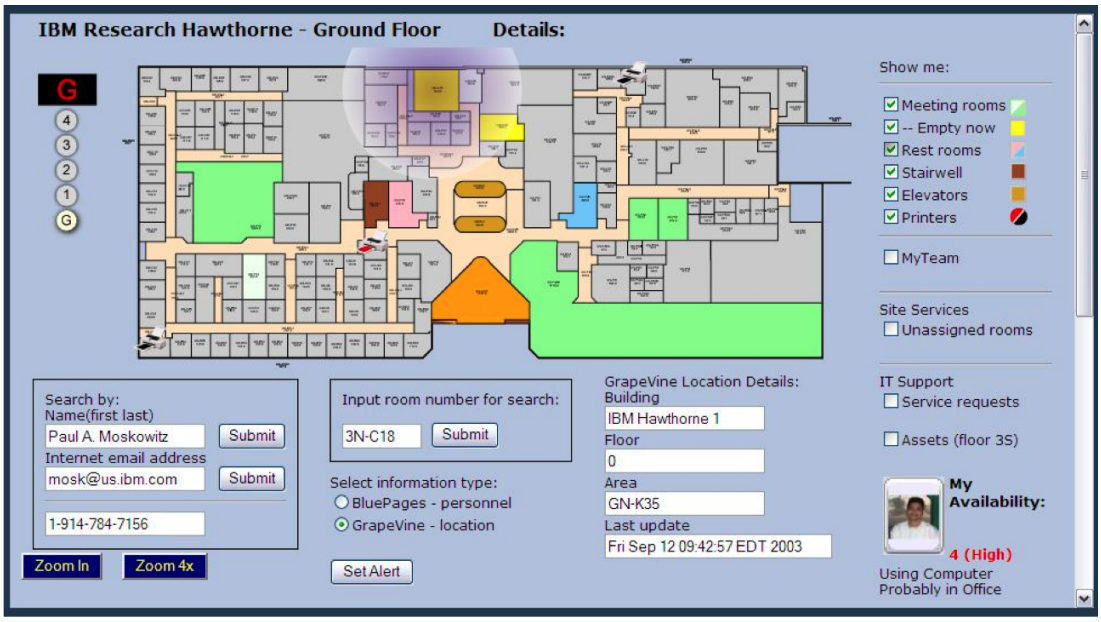


Figure 7.1: MySpace displaying the current location of a colleague

applications.

## 7.1 MySpace

MySpace (see Figure 7.1) is a browser-based interactive visualization of a user's physical workplace that provides dynamically updated information about people, places, and equipment. Users maintain a list of contacts (or "buddies" in IM terminology). For each contact, there is an associated set of permissions granted to the user by that contact. For example, if Sally has Paul in her team list, Sally will be able to view whatever information Paul has granted her permission for. Possible permissions include whether Paul's phone is off the hook, the location of the wireless access point that his laptop is connected to at work, whether he is connected remotely (if not in the building), which application he is currently using, and his IM activity. Additionally, a badge-based location tracking system is in the pipeline. Paul can choose whether to allow Sally to view all system-known information about him, or just a subset.


Figure 7.2: An e-card showing context with one-click communication links

In Figure 7.1, 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. 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 mySpace 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.

MySpace allows users to view the location of fixed resources (e.g., conference rooms, printers), mobile equipment (e.g., laptops) and to interact with them. For example, once a user has located the closest printer to his or her current location, clicking on the printer will take him or her to the Web page for setting up 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 (Richards and Christensen, 2004). An e-card (see Figure 7.2) is a means of initiating one-click communication.

### 7.1.1 Communication Channels

The e-card provides access to co-workers via phone, IM, or email. Alternatively, face-to-face meeting time can be requested via the calendar. Email support is provided by spawning a mail client, and IM 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 all employees.

### 7.1.2 Contextual Information

MySpace uses a set of rules and data about the user (speech detection, location, computer activity, and calendar entries) to model a user's availability for communication (Fogarty et al., 2004) on a scale of one to four, with 1 representing highly unavailable for communication and 4 representing highly available (Fogarty et al., 2004). When people are highly available (level 4), their image is shown in full color and their image becomes progressively grayer as their availability for communication goes down. It should be noted that the image itself is fixed and not a dynamically updated video snapshot as has been used in other awareness applications (e.g., (Dourish and Bly, 1992)). The only thing that changes is the degree of fading of the image based on the calculated availability for communication. Wired and wireless network connectivity is used to estimate location. For instance, if a person is currently on a virtual private network or dial-up connection, "remotely connected" is displayed below the image. Or if a person is connected from the access point that the person uses most often, he or she is labeled as "probably in office."

## 7.2 Study

It is well-established that users may be willing to give up privacy if provided with the appropriate incentives (Grudin, 1988). However, preferences regarding when and where one might choose to reveal which aspect of private information to whom and to what extent, had not yet been systematically studied. In an evaluation of a ubiquitous computing system with five undergraduate students at Berkeley, (Lederer et al., 2003c) found manual configuration by users to be 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 of how users define permissions for mySpace, we included a larger and more diverse sample of 36 users. Also, our focus was on supporting workplace activities, especially loosely coupled ones.

In order to better understand how people might achieve an appropriate reconciliation between privacy and awareness when using mySpace, we asked users to configure permissions for disclosure of their personal information. We were primarily interested in exploring two aspects:

1. Extracting commonality (if any) in how people configure privacy settings in order to inform appropriate default settings for mySpace.

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 formidable list of personal information (see Figure 7.3) would cause users to define more conservative permissions (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

| **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.**<br>**(Note that mySpace knows and displays current information only, and does not record or process historic information.)** | |
|---|---|
| **Location** | Whether you are at work or home<br>Work building in which you are currently located<br>Floor on which you are currently located<br>Room in which you are currently located |
| **Calendar** | Titles of all entries in your calendar (except for those marked private)<br>Times of all entries in your calendar (except for those marked private)<br>Locations of all entries in your calendar (except for those marked private)<br>Descriptions of all entries in your calendar (except for those marked private)<br>Participants of all entries in your calendar (except for those marked private) |
| **Instant Messaging** | Whether you are online or offline<br>Current IM status message<br>Number of IM conversation windows currently open<br>Amount of time elapsed since last IM conversation |
| **Activities** | Currently active application<br>Whether your phone is on or off the hook<br>Amount of time elapsed since keyboard or mouse activity was last detected<br>Whether speech is detected near your computer (and for how long) |

Figure 7.3: List of all pieces of context available to mySpace

comfortable enough to define permissions that allowed greater sharing.

### 7.2.1 Participants

Participants were recruited by requesting volunteers among permanent employees and summer interns in the research division of a large corporation. A total of 36 participants took part in the study – 24 permanent employees and 12 interns. Since mySpace is designed for supporting collaboration in the context of the workplace, the sample is representative of the target audience for such systems. Summer interns were specifically included to increase the variability of our user sample. Interns are much younger and less ingrained in the "organizational culture." Eleven out of twelve interns were between 20-30 years old, while only two permanent employees were younger than 30. The overall age distribution was 36% between 20-30, 25% be-

tween 31-40, 17% between 41-50 and 22% between 51-60. Participants were informed that we were studying mySpace but were not told that we were specifically looking at privacy aspects so as not to bias their perceptions regarding these aspects of the system. The study lasted about 45 minutes, and each participant was provided with a lunch voucher as a token of appreciation.

### 7.2.2 Methodology

The study itself consisted of three main parts.

1. **Part 1 – Demonstrating mySpace:** In the first part, participants were familiarized with mySpace by means of a demo/overview highlighting its various features and illustrating the 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.

2. **Part 2 – Performing Tasks:** We then asked participants to perform a set of ten tasks (identical for all participants), which were selected as representative of typical situations encountered at work. This allowed participants to acquire first-hand experience with mySpace, and provided a good opportunity for them to discover both the potential benefits and possible privacy intrusions implicit in an awareness application. We felt that understanding potential benefits of awareness information would provide an incentive for participants to appropriately manage the trade-off between revealing information about themselves, and preserving privacy.

Table 7.1: Descriptions of configuration modes

| | |
|---|---|
| **Global** | One set of global permissions applies for everyone in the company. |
| **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 company. |
| **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. |

Each task was phrased as a question. 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 the answer for the task, which was checked for accuracy by the experimenter before proceeding to the next task.

3. **Part 3 – Configuring Permissions for Aspects of Awareness:** 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 permissions could be configured in one of four (mutually exclusive) modes: Global, Team, Groups, or Individuals. They were provided with descriptions of each mode (as shown in Table 7.1), and were asked to choose the mode which best fits their needs and practices.

Table 7.2: Available levels for permission settings

| | None | Low | Mid | High |
|---|---|---|---|---|
| **Value** | 1 | 2 | 3 | 4 |
| **Location** | No info | Building | Floor | Room |
| **Calendar** | No info | Busy/Not busy | Titles | Activity details |
| **IM** | No info | Online/Offline | Status message | Activity details |
| **Availability** | No info | Available/Not available | Scale (1-4) | Activity details |

Once they had selected a mode, participants worked on their own to configure permissions for "when at work" and for "working from home." Each of the two was further subdivided into permissions for business and non-business hours (i.e., evenings, weekends, and holidays). In the existing corporate culture, remaining at work after business hours, or working from home is not uncommon. Participants specified permissions for location, calendar, IM and availability for communication. For each of these aspects of awareness, participants had to choose one of four levels of awareness corresponding to none, low, medium, or high (see Table 7.2). Participants who picked the Global mode were asked to configure a single set of permissions for everyone within the company, while those who picked the Team mode were asked to configure one set of permissions for their team, and another for everyone else in the company. Participants who picked the Groups 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 (i.e., "none") 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 permissions, participants completed an online questionnaire which asked questions aimed at gauging inherent attitudes towards privacy and trust. We selected questions from previous questionnaires on privacy (Cranor et al., 1999; Harris & Associates and Westin, 1998) and trust (Jarvenpaa et al., 1998; Rotter, 1967). The questionnaire also gathered feedback on participants' opinions regarding privacy

aspects of mySpace along with demographic information. At the end of the study, the experimenter conducted brief, semistructured exit interviews regarding the configuration activity (which included probing about the choice of configuration mode).

### 7.2.3 Study Conditions

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

1. **No disclosure, no feedback:** In this condition, participants received no explicit disclosure of pieces of personal context to which the system has access, nor were they shown any feedback/confirmation regarding the permissions they defined.

2. **Disclosure but no feedback:** In this condition, before starting the configuration activity, participants were shown a list of all pieces of personal context to which the system had access (see Figure 7.3). However, there was no feedback/confirmation after configuring permissions.

3. **Disclosure and feedback:** In this condition, before starting the configuration activity, participants were shown the same list as in the previous condition. In addition, after completing each configuration screen, an additional feedback/confirmation screen (see Figure 7.4) showed in tabular form, how the configured permissions would result in different aspects of awareness being shared with various contacts in the list. The screen provided the option to return to the previous configuration to make changes, if necessary.

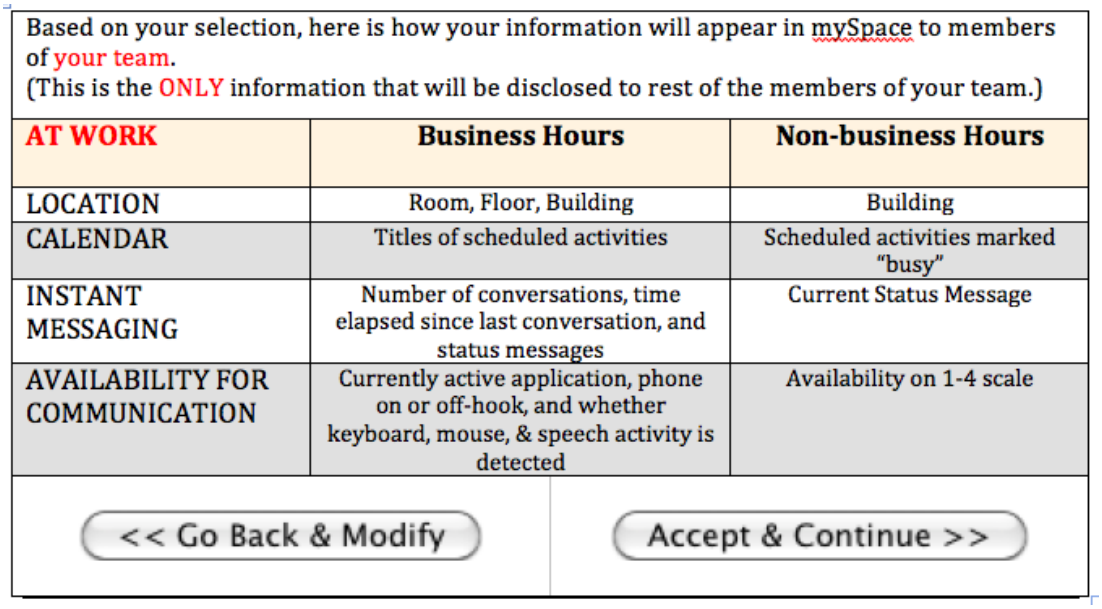


Figure 7.4: Feedback and confirmation of configuration

Participants were randomly assigned to one of the three conditions (we ensured an approximately even distribution of permanent male and permanent female employees, and male interns and female interns assigned to each condition). Of the 36 participants, 12 were assigned to condition 1, 13 to condition 2, and 11 to condition 3. Only the third part (configuring permissions) varied by condition.

## 7.3 Findings

A majority of participants ($\sim$ 70%) chose to configure permissions in the "Groups" mode. Permissions granted to various groups were significantly different from each other. Location was the most sensitive aspect of awareness. However, participants were comfortable disclosing it to colleagues on their team while at work during business hours. More privacy was desired after business hours even in a company with a culture of flexible work hours and occasional telecommuting. Contrary to expectations, explicit upfront disclosure of all pieces of personal context to which the system

has access, did not seem to induce more privacy preserving settings.

### 7.3.1 Preference for Groups

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

Participant feedback indicates that the preference for Groups was driven primarily by the fact that it provides enough flexibility for controlling access to personal information, without requiring too much burden to set up and configure. Participants indicated that Global and Team modes weren't flexible enough, while Individuals mode required configuring more details than necessary. They 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 IM contact list into groups as well. However, even participants who did not group their IM contacts selected Groups mode of configuration because of the greater sensitivity of the information involved in mySpace.

Majority (15) of the 25 participants who chose Groups created 4 groups. The rest specified between 2 to 5 groups. The average number of groups specified was 4. We believe that in actual use, without the burden of having to specify all groups at once, the number of groups created would probably be slightly higher than in the study. We found a lot of commonality among group definitions. Typically, specified groups

exhibited a concentric circle pattern with less and less awareness being shared as one moved away from the center. In some cases the center was "family" and in others it was "team."

To compare user permissions across groups, group labels created by participants were coded independently by two coders into the following categories: team, family, friends, collaborators/department, managers, others, and rest of the employees in the company. (To clarify, "team" is typically comprised of individuals with whom one works together closely on one or more projects with significant daily interaction. On the other hand, "collaborators/ department" includes individuals with whom one may be involved in a relatively smaller and looser collaboration with less frequent interaction.) In most cases, the coding was quite straightforward as participants used labels such as "My Team," or "Family Members." In some cases, knowledge of the company 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 employees in the company (from now on referred to simply as "Rest"), we added this group for comparison purposes. In these cases, all permissions for the added Rest group were set to "none" (since participants were informed that anyone not explicitly included in a group received no awareness information as 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 Groups mode with group 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 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 location and time of the calendar entry (and not current location and time of the user). As a result, findings for calendar permissions are somewhat meaningless and have been excluded from the analyses. As a final clarification, it should be mentioned that 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 this aspect were asked to ignore the current limitations of the system when configuring location permissions for the home.

### 7.3.2 Permissions between Groups

We found many statistically significant differences in the permissions granted to various groups. In particular, regardless of time and place, the group Rest was granted significantly lower levels of sharing when compared to other groups. Mean sharing for all three aspects of awareness ranged between 1 (none) to 2 (low). Not surprisingly, family received high levels of sharing regardless of place or time with means ranging between 3 (medium) and 4 (high) for all aspects (see Table 7.2 for descriptions of values). Most interestingly, during business hours the Team group (N=13) was granted the same levels of sharing as family (N=33) (see Table 7.3). Paired-samples t-tests for comparison of mean permissions for family and team were not statistically significant. The only exception was location information when working from home. Participants were willing to share with team members that they were at home (i.e.,building-level information) but not information at the floor or room level.

Table 7.3: Comparison of means for permission levels granted to Team and Family groups during business hours

| | **Location** | | **IM** | | **Availability** | |
|---|---|---|---|---|---|---|
| | **W** | **H** | **W** | **H** | **W** | **H** |
| **Team** | 3.76 | 2.00 | 3.12 | 3.15 | 3.27 | 3.09 |
| **Family** | 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 |

### 7.3.3 Permissions for Business and Non-business Hours

As expected, we found that more privacy is desired during non-business hours – both at work and at home (with the exception of family). Compared to the corresponding permissions for business hours, all groups (except family) received lower sharing during non-business hours – regardless of the user's location. As can be seen in Figures 7.5 and 7.6, sharing for team members, collaborators, and managers decreased significantly during non-business hours. Identical patterns were seen for the other aspects of awareness.

### 7.3.4 Permissions for Work and Home

Unlike time, place of work (either office or home) did not have a big impact on levels of sharing (see Figures 7.7 and 7.8). Additionally, sharing for IM awareness was high even for groups far from the core (e.g.,collaborators).

### 7.3.5 Variable Sensitivity for Various Aspects of Awareness

Some aspects of personal information are more sensitive than others. In our study, location seemed to be the most sensitive, while IM seemed to be the least sensitive.

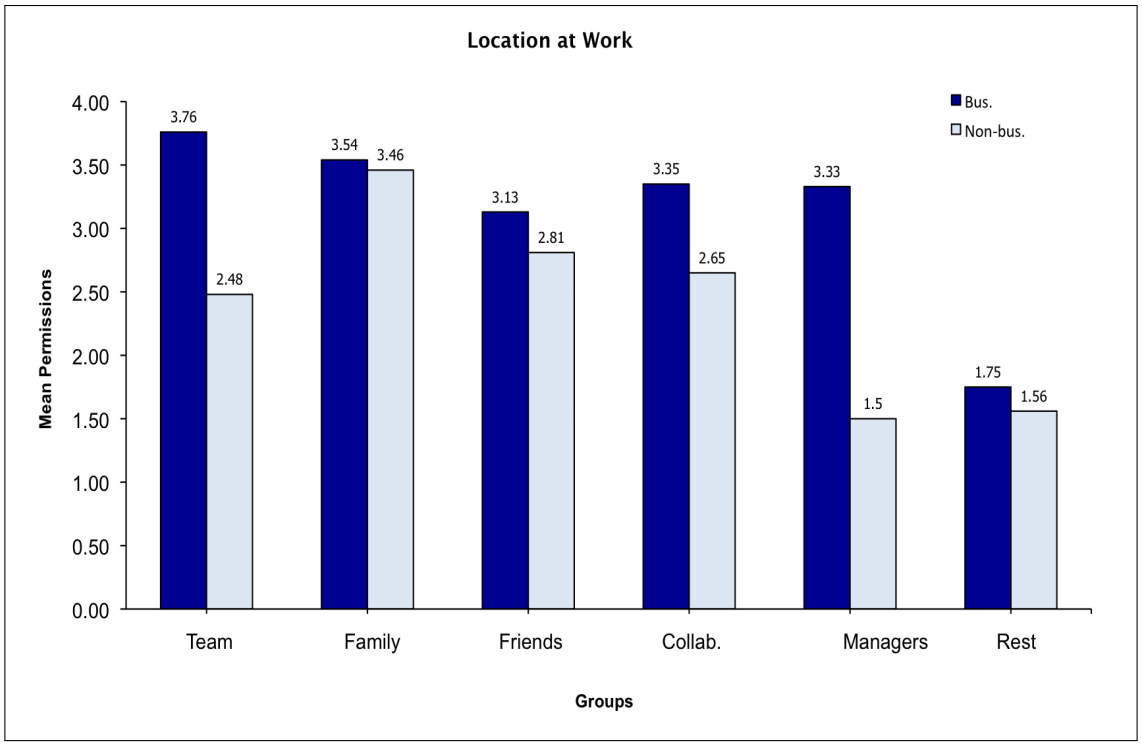


Figure 7.5: Comparison of means for permissions granted to groups for location information at work

This is evident from relatively large differences in permissions for location based on both time and place (see Figure 7.9 and 7.10). Additionally, participants were a lot more reluctant to disclose details of their location at home, whether during or after business hours. Permissions for IM, on the other hand, remain constant and at high levels of sharing.

### 7.3.6 Effect of System Disclosure and Feedback

Contrary to our hypothesis, disclosing a detailed list of all pieces of personal context to which mySpace had access did not lead to more privacy-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. In fact, we were surprised to observe more sharing of availability awareness with team in

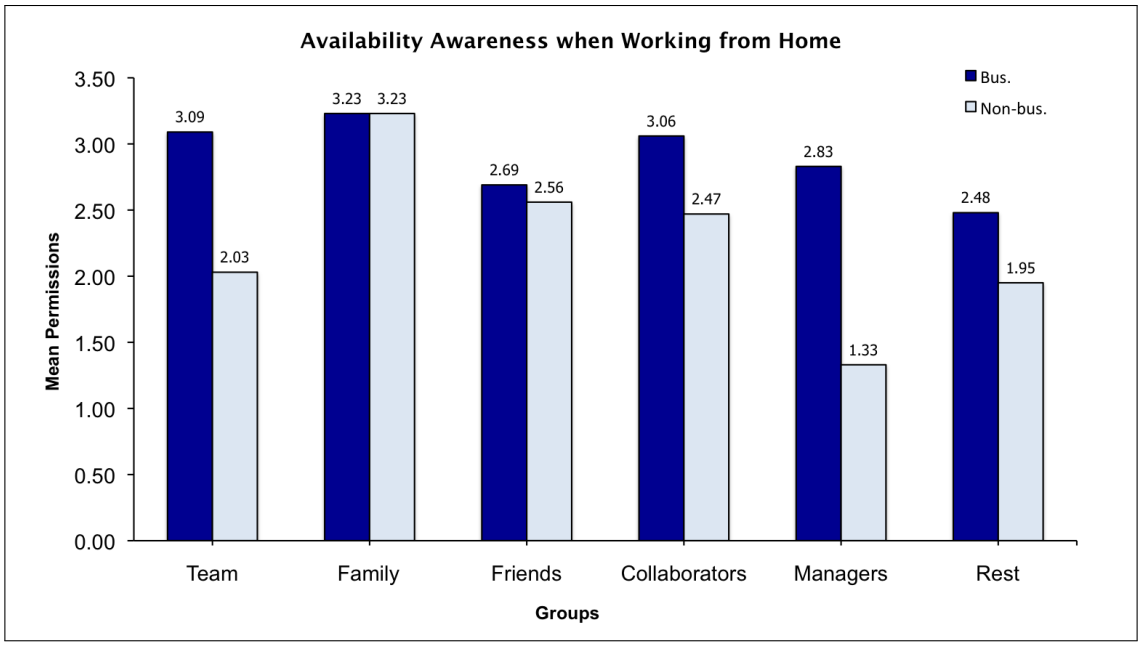


Figure 7.6: Comparison of means for permissions granted to groups for availability awareness at home

Condition 2 both at work (M2 = 3.64, M1 = 2.73, $p < 0.005$) and home (M2 = 3.36, M1 = 2.55, $p < 0.005$). Other factors such as availability permissions for friends, IM permissions for collaborators were nearing statistical significance ($0.1 > p > 0.05$) for higher sharing in condition 2. As stated earlier, not all participants created the same number of groups. For instance, while almost every participant specified a "team" group, only six created a "manager" group. It is likely that a larger sample size would have led to statistically significant differences for these factors.

We had expected that permissions would move towards greater awareness sharing in Condition 3 (with feedback/ confirmation) than in Condition 2. However, we found no significant differences. This could be because the feedback was provided after participants configured permissions. Real-time feedback with a visual component (rather than our tabular interface) may have achieved a more significant impact. The lack of statistical significance may also be due to the small sample size for some of the groups (e.g., only 6 participants defined a Manager group).

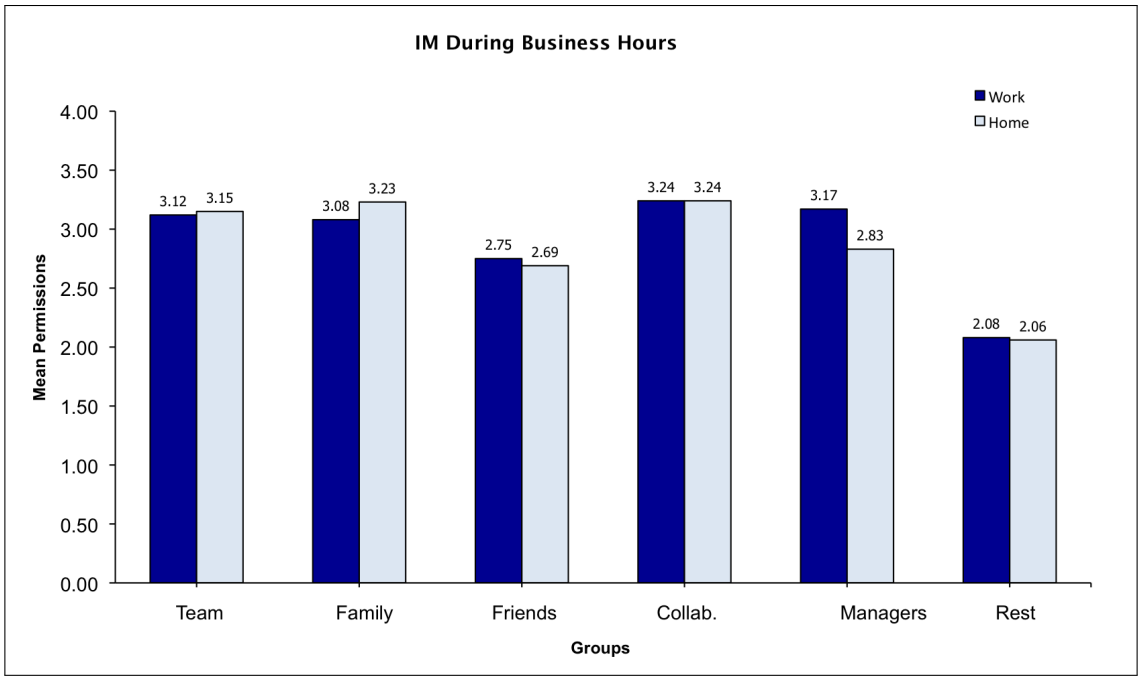


Figure 7.7: Comparison of means for permissions granted to groups for IM during business hours

### 7.3.7 Inherent Privacy Preferences

Based on 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. The range of variability among our participants regarding inherent privacy and trust attitudes was not very wide. The privacy index ranged from 0.52 to 0.87. Thus all of our participants can be considered "privacy pragmatists" (i.e., choosing to take a pragmatic approach to privacy issues based on the situation rather than being unconcerned or overly concerned in all cases) (Cranor et al., 1999). There were no significant differences in permissions based on the privacy index. Nor was there any significant impact due to organizational culture.

We looked for differences between permanent employees or summer interns, and again found nothing of interest except that summer interns tended to share less availability

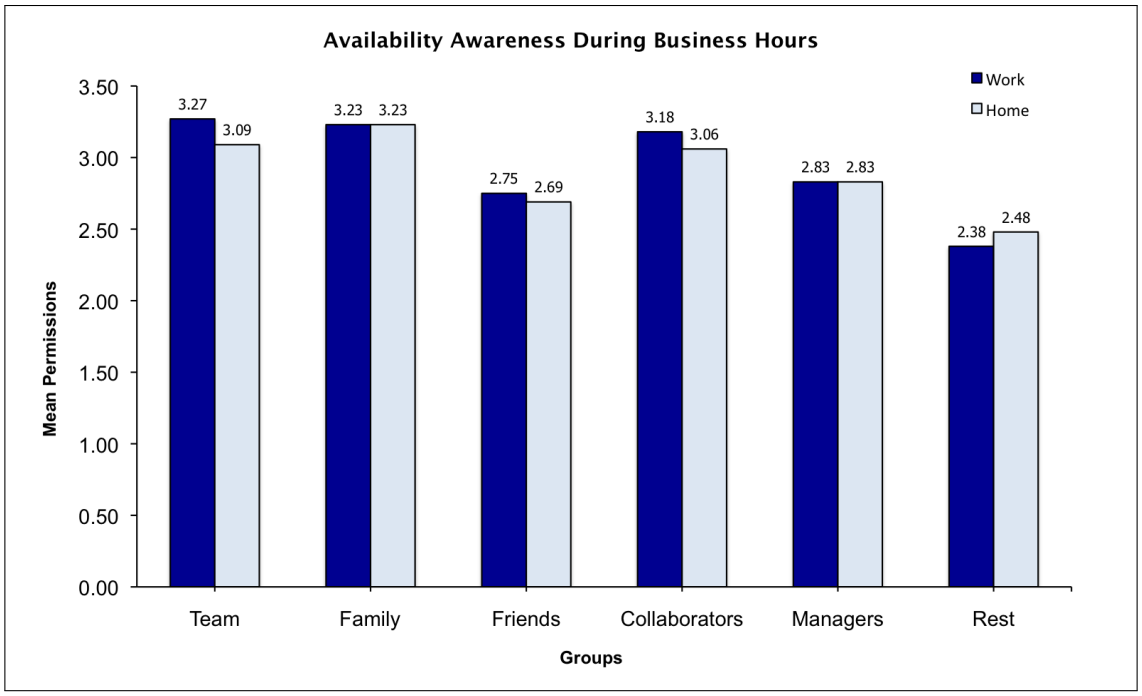


Figure 7.8: Comparison of means for permissions granted to groups for availability awareness during business hours

information with managers when at work after business hours ($p < 0.001$). Finally, we did not detect any major effects based on gender or nationality.

## 7.4 Discussion

Understanding how users achieve an effective reconciliation between privacy and awareness involves studying how they configure permissions for an IAIS initially, as well as how these settings change over time. In this study, our aim was to understand how best to help users with the initial configuration task. Given that user proficiency with the system increases over time and that context changes (e.g., team configuration change), it would be interesting to run a longitudinal study to understand if, and how, users modify initial settings.

The configuration of permissions in our study is similar to the personalization of

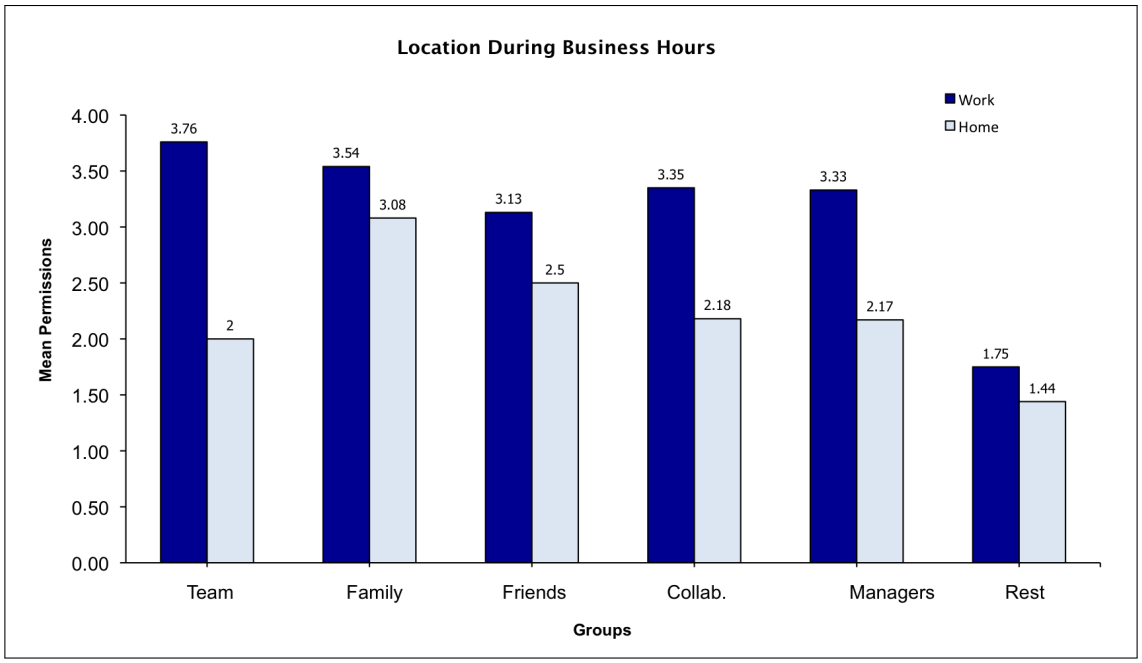


Figure 7.9: Comparison of means for permissions granted to groups for location during business hours

default settings when installing a piece of software for the first time. As noted earlier, one of the goals of the study was to understand how to reduce this burden by getting the defaults right. In future work, we would like to examine the types and the frequency of changes to the initial settings during an extended pilot study. Such a study would also provide an opportunity to verify the effectiveness of various interface mechanisms proposed in the previous section.

Reciprocity is often as an important privacy control feature in a media space (Bellotti and Sellen, 1993). However, the concept of reciprocity was not applicable in our study since the user explicitly allowed a colleague access to his or her information. These permissions were granted without regard to the permissions that colleague had granted the user (or even whether any permissions had been granted by the colleague at all).

Although findings presented in the paper are within the context of mySpace, it should be noted that mySpace is a portal that provides unified access to various applications

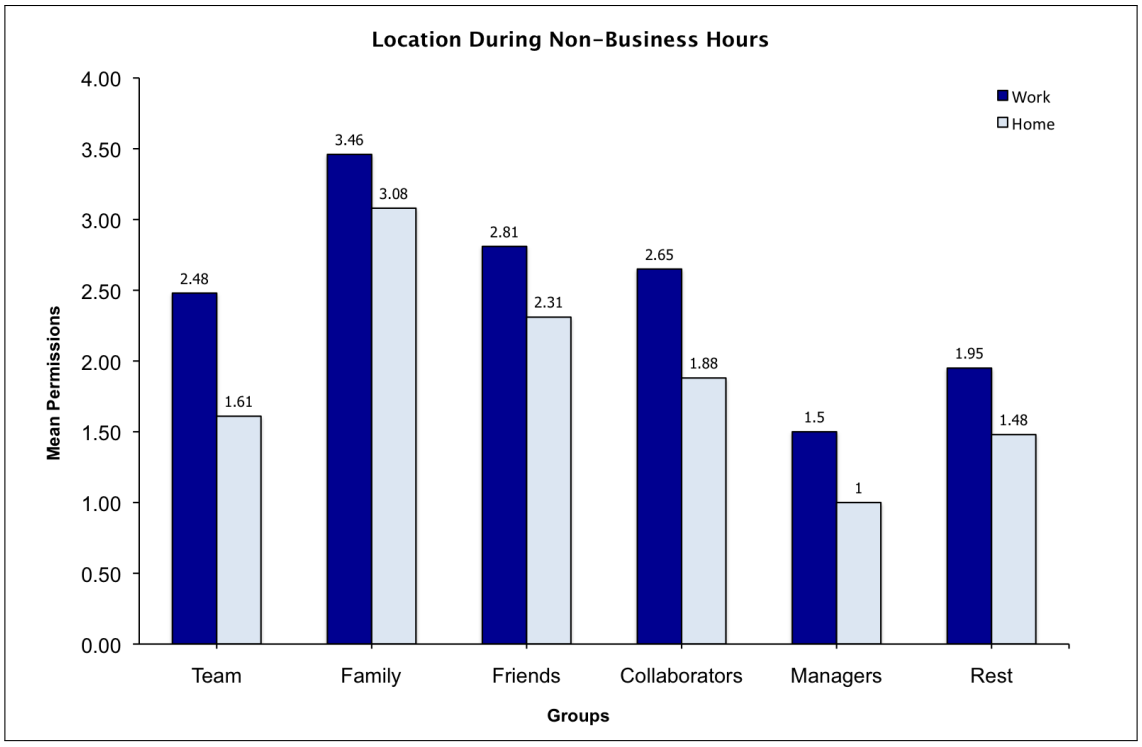


Figure 7.10: Comparison of means for permissions granted to groups for location during non-business hours

such as email, calendar, and IM by utilizing their APIs (Application Programming Interfaces). It is relatively straightforward to extend mySpace to include information from other applications that provide context information (e.g., an Active Badge system). Also, mySpace presents the same aspects of awareness (location, calendar, IM, etc.) that are available in many other awareness applications. As a result, we believe that the findings are applicable beyond mySpace and could shed light on user preferences for privacy settings in other IAIS operating within a corporate work setting with similar components (i.e., location, calendar, IM, and availability).

## 7.5 Implications

Our findings provide strong support for providing grouping functionality in IAIS for more than contact list organization. Defining permissions at the group level appears to provide the flexibility needed to reconcile privacy and awareness without undue burden. Configuration burden could be further reduced by providing templates of settings for commonly used groups such as Team, Collaborators, or Family. Defaults for templates could be based on a quick user study of the target population (or 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 (Lederer et al., 2004). Since majority of users rarely modify default settings, getting defaults right ensures an appropriate privacy-awareness setting from the outset. Even if only 75-80% of the defaults are appropriately set, the user is perhaps more likely to fine-tune the rest. 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 could undermine the awareness benefits of the system.

Many participants expressed the desire to have the ability to copy settings from another group, and make changes to that copy. This desire also seems to reflect the underlying concentric circle pattern mentioned in the findings. Providing a global template that groups can inherit from, or allowing the functionality to copy the settings from a pre-existing group also seem like useful solutions for reducing the configuration burden without forfeiting flexibility. Further, automatic (or semi-automatic) adjustment of settings to accommodate differences for business and non-business hours could also help.

While user sensitivity to room-level location being broadcast from the home is not surprising, system builders of location-aware systems will be heartened that during working hours users are not averse to sharing their location with colleagues considered to be part of their team. The mode of permission for team members during business hours was 4 (i.e.,room-level location) – the highest possible setting. If designers provide greater user control over more sensitive aspects of awareness, users may feel comfortable enough to appropriately share such information via the system.

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 in the same company, 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 some access to oneself even when at work. Of all participants who chose Groups 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 would also have created these groups, but may not have done so due to the assumption that mySpace was only designed for the employees of the company.) The question of how exactly non-organizational personnel can be incorporated in a workplace system is one open to further research.

Disclosing a detailed list of all pieces of personal context collected by the system does not seem to scare users into choosing more privacy-conservative settings. In fact, it appears as if such a disclosure may act as a trust-builder, reassuring users to reveal more information to the colleagues on their team (Moore et al., 1999). Our table-based feedback/confirmation interface designed for alleviating user privacy concerns, seems not to have been effective enough. 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. Even today, in many organizations the use of IM is either completely prohibited, or severely restricted. Our findings suggest that organizations may wish to re-evaluate whether they are likely to benefit by promoting an organizational culture in which use of IM is encouraged.

# Chapter 8

# Field Study of a Geographically Distributed Software Development Project

To further broaden the scope of our investigations, we engaged in a field study of a software development project called "Project X." The goal of the investigation, described in detail below, was to look at the reconciliation of privacy and awareness needs as they occur in collaborative work practices in general, regardless of which specific tools, applications, or systems were utilized.

## 8.1 Methodology

Project X was spread across five sites of a large multinational telecommunications corporation. Our objective was to investigate how individuals engaged in geographically distributed collaboration satisfy their awareness and privacy needs. The bulk

of the study was conducted over a period of approximately 10 weeks during which one member of the research team was based at one of the Project X locations as a summer intern. An initial hour-long conversation with the head of Project X helped us gain basic understanding of the project in order to devise a methodological plan. Thereafter, we used the methods described in the following subsections.

Two points must be emphasized:

1. To avoid biasing the participants, the advertised goal of the research was to study collaborative work practices. Our focus on privacy was not revealed to anyone outside the research team (not even to the head of Project X)[1].

2. We did not provide a definition of privacy for the study participants. Instead, we asked *them* to explain what "privacy" meant to them in the context of their work and work practices. Our intention was to avoid imposing any specific notion of privacy on the participants. Instead we sought to uncover the various contextual meanings that they associated with this concept as well as to uncover their work practices aimed at meeting their privacy needs.

### 8.1.1 Non-participant Observation

Our exploration started with non-participant observation of the meetings of the Project X management team. These meetings were mainly used to formulate the detailed plan for upcoming activities. Managers from all project sites and all hierarchical levels participated in the meetings. Typically, about six to eight participants from the site where we were situated gathered in a conference room, while those from other locations joined in via a Web-based conferencing system. This system

[1]At the end of the study, we sent a "closure" email to all participants that described the real goal behind the study.

allowed one to use the phone for audio and the Internet for watching or delivering presentations. The system also showed a list of all meeting participants with a visual indicator showing the person(s) currently talking. In the conference room, the presentation material was also projected on a screen in the room. Moreover, the individual participants sometimes engaged in "back-channel" IM conversations.

We observed five such meetings. At three of these meetings, the researcher was present in the conference room. The other two times he participated "remotely" using the Web-based conferencing system, once from his office and once from an off-site location. The former was chosen to experience the situation faced by those who called in from their offices while the latter was meant to recreate the experience of telecommuters. These observations helped us gain further understanding of the organization and the activities of the project. This understanding was used to guide further methodological choices.

Our rationale for observing the meetings was threefold: (a) to facilitate our access to the project by getting introduced to the whole management team (see Section 8.8.1), (b) to gain an understanding of the larger context, organization and workflow of the project (see Section 8.2), and (c) to make up for not shadowing individual project members (see Section 8.8.7) by observing a group as it engaged in actual work practices.

### 8.1.2 Site Visits

Two members of the research team were based at one of the sites of Project X located on the East Coast of the U.S. We also visited three of the other sites: one in the mid-U.S., one on the West Coast of the U.S. and one in India. About a week was spent at each of the three sites conducting interviews with individual contributors

(see below) as well as observing site-specific factors such as architecture, layout, work practices and culture. Photographs of the sites were also taken in order to share the observations with the researchers who did not visit the sites (see Figure 8.1). Additionally, we procured site-specific information such as the total floor space, office sizes, and occupancy. Although we did not visit the fourth site (also located on the East Coast of the U.S.), we interviewed two contributors from this site while they were visiting the site at which the research team members were based.

### 8.1.3 Semi-structured Interviews

Across all sites, we conducted semi-structured individual interviews with fifty-two Project X contributors. The interviews lasted about 90 minutes on average. The topics for the questions were derived from our research objectives and were divided into three main themes: general information on work practices, needs for awareness and privacy, and opinions on enhancements to existing collaborative tools. We used the information from our initial conversation with the head of Project X, as well as the insights from the above-mentioned observation of the management meetings, to tailor the questions to the context of Project X. Additional understanding gained from the first few interviews was used to further extend and refine the set of questions. This set was then used with little modification for all remaining interviews.

To the extent possible, we selected interviewees in such a way as to achieve broad coverage across the different job functions (see Section 8.2.3) at the various sites (see Table 8.1. To avoid biasing others, interviewees were asked not to discuss the interview with other employees in the corporation (including their managers). In all but six cases, the interviews were audio-recorded for later transcription and analysis. The other six individuals refused to grant permission to audio-record. In these cases,

Table 8.1: Project X interviewees at the different sites based on job functions

| Job | East Coast 1 | East Coast 2 | Mid-U.S. | West Coast | India | TOTAL |
|---|---|---|---|---|---|---|
| Upper Management | 1 | 1 | – | – | 1 | 3 |
| Manager | 3 | – | 2 | 1 | 1 | 7 |
| Developer | 5 | – | 9 | 5 | 5 | 24 |
| Tester | 2 | – | – | – | – | 2 |
| Systems Engineer | 2 | – | 1 | – | – | 3 |
| Architect | 1 | – | 1 | 1 | – | 3 |
| SCM | 2 | – | 1 | 2 | 1 | 6 |
| Other | 2 | 1 | – | – | 1 | 4 |
| TOTAL | 18 | 2 | 14 | 9 | 9 | 52 |

we took detailed handwritten notes. The majority of the interviews were conducted by one member of the research team. For some of the interviews at the East Coast site one of the other research team members accompanied him as a secondary interviewer.

When possible, the interviews took place in the office of the interviewee. In shared office or cubicle situations, we used nearby conference rooms or empty offices. The goal was to interview people as close to their regular work area as possible, so that they could point out relevant information and artifacts on their computer screens, in their offices, and along their hallways[2]. This was important because prior research has found that individuals sometimes reconfigure their workplaces to suit their preferences and practices (Dourish et al., 2004).

Transcripts of the interviews were analyzed using the grounded theory approach (Glaser and Strauss, 1967). Categories that emerged from open coding were further refined into ten higher-level categories by selective coding. Then, axial coding was employed to identify the relationships between these higher-level characteristics resulting in a framework (see Section 8.3 that illustrates how privacy management operates in the collaborative work context.

[2]Several interviewees did comment on these aspects during the conversation. A few also showed us information on their laptops.

### 8.1.4 Online Questionnaire

Based on the understanding gained from the above activities, we next formulated a questionnaire (see Appendix B). The questionnaire was administered online a few months after the conclusion of the other methods described above. It aimed at delving deeper into important aspects uncovered during the interviews and site visits. These included interruptions, trust, impression management, and customization of technology to fit personal preferences and practices. The survey also enabled us to achieve broader coverage across Project X by reaching those whom we had not been able to interview. In addition to questions regarding Project X and work practices, we also used scales from the literature for measuring privacy (Westin, 1991; IBM, 1999), team trust (Jarvenpaa et al., 1998), interpersonal trust (Rotter, 1967), and self-monitoring (Snyder, 1974) and asked for demographic information. The questionnaire was distributed to all Project X members (125 at the time of the questionnaire deployment). We obtained 90 valid responses, yielding a response rate of about 74%. When the questionnaire was conducted some of the individuals we originally interviewed no longer worked on Project X due to attrition or organizational restructuring. Thus, we were able to gather responses from only 30 of our original 52 interviewees.

## 8.2 Setting

To set the stage for the discussion that follows, we describe the setting of Project X in detail. Our methodology enabled the rich understanding of the intricacies of the project along with its context and history. As the following discussion will show, it also allowed us to recognize and analyze the five types of boundaries – geographical, functional, temporal, identity, and organizational – outlined by Espinosa et al. (2003).

Project X involved roughly 125 employees spread across five different geographical locations: four in the U.S. and one in India. The project was tasked with building a middleware platform that would provide its services in the form of a well-defined API (Application Programming Interface). The goal was to utilize the API as the framework underlying every higher-level application software built by the corporation. As a result, the task of Project X was not only complex and challenging, but it also held organization-wide significance due to the involvement of a variety of stakeholders.

### 8.2.1 Software

Project X did not start from scratch in its endeavors. Various pieces that needed to be integrated into the middleware platform already existed as separate entities in a variety of forms. In fact, Project X was conceived with the explicit goal of unifying these disparate pieces into a homogenous, streamlined platform in order to reduce code duplication across the corporation and to simplify the task of those building higher-level application software and hardware.

During the course of our study, the platform comprised of eighteen modules integrated into a single release. Due to the interdependencies between the modules, a release could however not be created by merely lumping the modules together. As a result, frequent cross-module collaboration was required in all phases, i.e., architectural design, development, testing and integration. The amount of dependency, and thus the extent of the cross-module collaboration, varied from module to module. A few modules were relatively independent while some others were heavily dependent on several other modules. For instance, the module that was tasked with the installation of the release needed to handle the installation of every module and thus depended on *all* other modules. Collaboration was also required during *knowledge transfer* phases

whenever there was a change in the individuals or the team responsible for a module.

Collaboration spanning the entire project was also needed for planning and coordination purposes. The management (from multiple managerial levels) worked together on planning project activities, tracking progress, making adjustments, and setting future goals using estimates and forecasts. The Source Code Management (SCM) unit provided services to Project X to manage the repositories of its source code. Representatives of the higher-level software products that would use the Project X platform (dubbed as "adopting products") were also consulted for requirements and feedback.

### 8.2.2 Workflow

Project X releases were arranged in *release cycles* of about three to four months. Every successive release incorporated new features, and fixed bugs from the previous release. Each feature or bug was treated as a Modification Request (MR) in the SCM system. As in any software project, each release cycle involved coding new features, fixing bugs, testing software units, integrating them, and testing the integrated release. During a release cycle, the management team tracked its progress and also developed the detailed plan for the next release. As per the organizational culture, the deadline for the final delivery of a release was never changed. This rigidity also applied to the various "internal" deadlines within the cycle. If the planned features could not be finished by the deadline, they were either pushed to the next release or were included despite the existence of known bugs. Such "rollovers" often had a cascading effect on subsequent release cycles.

### 8.2.3 Personnel

Due to its size, scope and complexity, Project X required contributions from a variety of people.

**Managers:** Several levels of management were involved in Project X. Upper management directed the overarching vision and goals, while lower management translated those goals into release cycles and tracked the progress of individual contributors. Each lower-level manager typically "coached"[3] a team of individual contributors who performed the different functions described further below. A project manager was responsible for maintaining an official detailed project plan used to schedule activities, and to record, track, and estimate progress. Finally, a "program manager" was responsible for ensuring that various phases of Project X were aligned with the organizational guidelines regarding large-scale projects.

**Architects:** Architects were responsible for the higher-level software design and for matching the architecture of the Project X platform to the business vision and goals of the organization.

**Systems engineers:** Systems engineers translated the architectural specifications into requirements for the individual modules. The requirement specifications went through several iterations based on feedback from the architects and the developers.

**Developers:** The core coding was done by the software developers. Multiple developers (typically from the same team) were involved in the development of each module. Linux was used as the development platform whereas the other work

[3]The organizational culture was to refer to one's manager as a "coach."

activities (such as email, or document editing) were carried out using Microsoft Windows®.

**Testers:** Once an initial module build was complete, testers were responsible for testing that the module conformed to the requirements and specifications, and for generating MRs as necessary. In addition to unit testing, testers were also involved in integration testing of the entire release.

**SCM support:** A sophisticated and robust SCM system was critical for Project X, as for any complex software project. This service was delivered by the unit that provided SCM services to the entire corporation. The unit was responsible for the smooth operation of the SCM system and for troubleshooting SCM-related problems.

**Customers:** Project X also sought involvement of the "adopting products." After all, these were the (internal) customers towards whom Project X was oriented. Representatives of these products provided their input primarily to the Project X management team and the architects.

It should be noted that not all of these project members spent 100% of their time on Project X. While most developers, testers and lower-level managers worked solely on Project X, other contributors were involved in (multiple) other projects. The percentage of time that these individuals spent on Project X varied from merely 3-4% to more than 50%. Additionally, the time spent was also dependent on the current phase within a release. Some phases required greater contribution from specific individuals. For instance, in some stages Systems Engineers spent nearly all of their time on Project X while during the rest of the period, their effort could be an order of magnitude lower.

Personnel changes also affected the operation of Project X. For instance, when we began our study, teams from Europe had just moved out of Project X. It was also not uncommon for the module assignments to be reshuffled among the various existing teams in different release cycles. Thus, a team that worked on a particular module during one release could find itself assigned to a different module in the next cycle. It was therefore difficult (even for the management) to pinpoint exactly who was involved in Project X, in what capacity and to what extent. In fact, we initially spent a great deal of time merely compiling a list of project members and their specific duties.

### 8.2.4 Locations

All of the personnel mentioned above were geographically distributed across five main locations: four in the U.S. (in three different time zones) and one in India. The number of people at each location varied from a handful to more than thirty. Interestingly, team[4] membership was independent of geographical separation. It was not uncommon for a team to be distributed across different locations. In addition, a limited amount of telecommuting was common in the U.S.. In a couple of cases, individuals worked out of their "home offices" the majority of time, coming to their workplace only as needed.

Notably, each site possessed its own history. For example, the U.S. West Coast site previously belonged to another company that was acquired by the multinational corporation. Many of the Project X members at this site had been working together for several years as employees of the previous company. Moreover, the sites also differed in features such as the area of offices, the height of cubicle dividers, the presence of a cafeteria etc. (see Figure 8.1). For instance, the lack of a cafeteria at the mid-U.S. site prevented Project X members from interacting over lunch as was

[4]We loosely define a team to be a group of individuals coached by the same manager.

Figure 8.1: Physical layouts of the Indian site (left) compared with those of the U.S. sites (right)

typical at the East Coast site. The U.S. sites were spacious (see bottom right picture in Figure 8.1), while the Indian site was densely packed (US: 419 sq. feet / person, India: 144 sq. feet / person). These architectural features had a noticeable impact on preferences, attitudes and work practices (see Section 8.7.1).

### 8.2.5 Collaborative Tools and Practices

Project X members used several communication and coordination tools for managing their collaboration:

**Email:** Email was used extensively by every project member, not just for communication but also for knowledge management and as a memory aid. Features of email such as vacation auto-replies or read-receipts were used for providing and seeking awareness of activities.

**IM:** IM was used a great deal by some members of the project only. In other cases, use of IM was sporadic, if at all. IM was generally utilized for:

- quick turnaround communication, which was mostly treated as ephemeral,
- avoiding phone calls to be able to multitask,
- circumventing problems in voice communication resulting from different accents,
- checking if someone was available for a phone or face-to-face meeting, and
- communicating on the "back-channel" during meetings and conference calls.

**Shared calendars:** Sharing one's calendar was the organizational norm. The shared calendars were used as the primary means for checking availability and scheduling meetings. Those involved in multiple activity spheres (González and Mark, 2004) (for example, those working on multiple projects) used calendars far more than others (such as developers). The default sharing indicated whether or not someone was busy during a given time slot without showing the details of the scheduled activity. Although sharing the details was an option, most people

did not modify the default, either because they accepted the it as is or because they deliberately chose not to share details.

**Microsoft Project®:** A project plan was created and maintained using Microsoft Project®. The plan was used to track progress by sending reminders, seeking status updates, adjusting estimates etc. Although the project manager was the person in charge of maintaining the plan, it was available for viewing by any project member.

**Telephone:** Many project members relied heavily on the telephone. Phone use for one-on-one calls was typically limited to urgent situations or matters for which written communication was unsuitable. More significantly, the telephone was critical for conference calls that involved multiple people at different locations. Sometimes, participants from the same site would gather in a local conference room. However, because conference call meetings were deeply rooted in the organizational culture, it was also not uncommon to have such conference calls where individuals participated from their offices, even when all parties in the call were situated at the same site. When people joined conference calls from their offices, they frequently multitasked and only attended to those parts of the calls in which their attention was required. As a result, it was a common practice to put the call on "mute" at all times except those during which one needed to speak.

**SCM system:** The SCM system provided valuable support not just for version control but also for keeping track of MRs. In addition, it generated reports and statistics to monitor project progress and make estimates for future planning. Each module was assigned a separate trunk within the repository and each developer working on a module was responsible for his or her own branch within the trunk. This limited the ability of others to see the changes in other modules

before the integration phase. Awareness of such changes, however, was important due to module interdependencies. In addition, developers were typically reluctant to merge code with the main trunk if they felt it could be perceived as "half-baked" or "incomplete." They did not wish to be judged as incompetent based on visible unpolished code, nor be responsible for breaking the build with their committed changes. As a result, intermediate "development" versions of the code were sometimes shared outside of the SCM system with the developers of dependent modules. The phases during which all modules were integrated was neverthless hectic and stressful, due to integration issues which invariably popped up.

**Document repositories:** Apart from computer code, various other documents produced by the project members could be shared with others via a Microsoft Sharepoint®document repository and an internal system for publishing documents for organization-wide distribution. These systems allowed one to store one's work and share it with appropriate team members to seek comments. It also served knowledge management and organizational memory purposes.

**Internet Conferencing:** In addition to telephone conferencing, there was occasional use of Internet-based conferencing such as Web-based conferencing and Microsoft NetMeeting®, as well as of remote desktop connection such as VNC (Virtual Network Computing).

## 8.3 Privacy Management Framework

Figure 8.2 shows the framework that emerged from our analysis (Patil et al., 2009). It presents privacy management practices in collaborative work as dependent not just on a number of situational characteristics but also on a hierarchy of personal

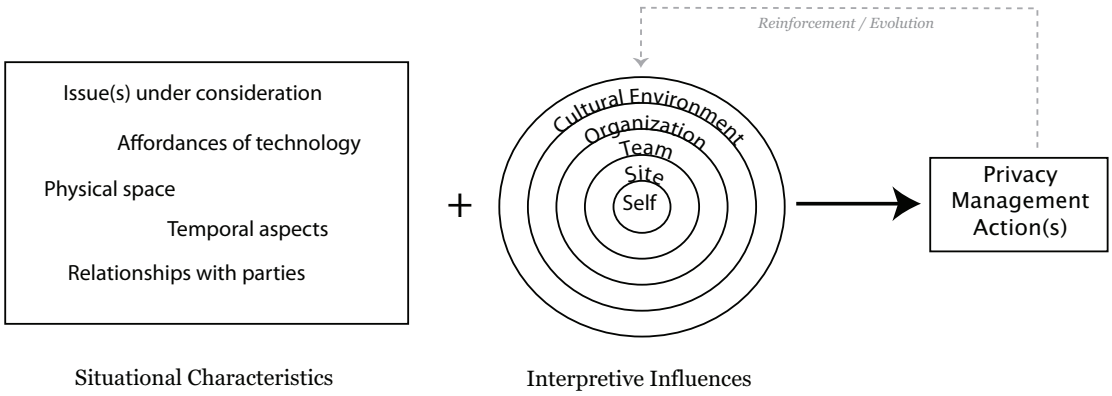


Figure 8.2: Privacy management described in terms of interpretive influences applied to situational characteristics

interpretive influences that an individual applies to the situation. As can also be seen in Figure 8.2, the interpretation applied by an individual to the situation at hand leads to privacy management action(s), or lack thereof. Moreover, these actions themselves form a feedback loop that contributes to the reinforcement and/or evolution of the interpretive influences over time. Privacy is known to be a context-dependent and highly personal concept (Palen and Dourish, 2003; Acquisti and Grossklags, 2006). The framework captures the former aspect in terms of the situational characteristics, and the latter through the interpretive influences. (The interpretive influences are related to the "identity" boundary whereas the situational characteristics encompass the "disclosure" and "temporal" boundaries described by Palen and Dourish (2003).)

### 8.3.1 Situational Characteristics

Our analysis revealed five key situational characteristics that interviewees deemed important when reconciling privacy and awareness needs.

**Issues:** The details of the issue(s) at hand were instrumental in judging aspects such as confidentiality, urgency, audience, or communication medium. These

judgments, in turn, affected privacy management actions.

**Relationships:** This characteristic refers to the nature of relationships – formal as well as informal – that existed among the various parties involved in a particular situation.

**Temporality:** Two temporal aspects impacted a situation. The first was the time of day in one's own time zone as well as in those of one's collaborators. The second was the temporal *extension* of the present action(s) into the future in the form of archives, logs, records, or people's memories.

**Technology:** As described in Section 8.2, collaborative activities utilized a host of technologies. The affordances as well as the limitations of a system constrained which actions it could support, and in what manner (Norman, 1988).

**Space:** This characteristic refers to the physical space in which work was carried out. It includes the design and layout of workspaces and work sites, and also of other locations from which individuals worked (such as homes, conference rooms, offices of others, cars, and hotels).

The situational characteristics Issues, Relationships and Technology map to and refine, respectively, the concepts System Properties, Actor Relations, and Information Types proposed by Lederer et al. (2003a). Similarly, Issues, Relationships and Temporality subsume Information Sensitivity, Receiver and Usage from Adams's (1999) model. Even though we discussed each of the characteristics separately above, a multiple of these often came into play in any given situation. In other words, all of them were subject to interpretation simultaneously. This is illustrated by the supporting examples in Section 8.4.

### 8.3.2 Interpretive Influences

While the characteristics described above set the stage, the privacy management action(s)[5] of each individual further depended on his or her interpretation of the situation. We identified five major influences that guided this interpretation.

**Self:** Individuals drew upon their personal disposition and characteristics when interpreting a situation.

**Team:** The practices, norms or policies of one's team were also crucial in deciding how situations were interpreted. We observed that the impact of this influence was dependent on factors such as the length of time the team members had worked together, the degree of work coupling, and the management style of the team leader.

**Site:** This influence refers to practices and local factors that were unique to a given site. For example, the typical practice at the U.S. West Coast site was to arrive at the workplace later in the morning than at the other U.S. sites.

**Organization:** The multi-national corporation was the umbrella uniting the different sites. It influenced the interpretation by providing policies and norms, a shared sense of identity, as well as a shared technical infrastructure for carrying out work activities.

**Cultural environment:** The cultural environment external to the organization in which one was embedded also influenced how situations were interpreted. The large differences between the privacy preferences and practices at the India site compared with those at the U.S. sites is one of the salient findings of the field

[5]The framework also treats inaction, i.e., deciding not to act, as an action.

study (see Section 8.6). These differences were partially attributed to the impact of the cultural environment.

We also noted that the above influences could be arranged in a hierarchy beginning with the most inward influence (self), and growing progressively outward toward the larger environment one is embedded in. The interrelationship between the influences also needs to be emphasized. For instances, differences between sites can be attributed not just to local factors (such as the history of the site, the interactions among local colleagues, the weather etc.) but also to organizational factors (such as policies or infrastructural variations) as well as cultural influences. In order to isolate the contribution of an individual influence, it may be necessary to make comparisons. For example, the cultural environment is unlikely to be a major contributor to differences among sites within the U.S.

## 8.4 Supporting Examples

In this section, we present four frequently encountered situations in which collaborators are faced with reconciling privacy and awareness: making communication[6] choices, handling interruptions, working from home, and dealing with urgent matters. The following subsections describe how the framework presented above explains the privacy management actions that we encountered in these situations (the labels in italics indicate the applicable situational characteristics and interpretive influences). Although we discuss the four separately, it should be noted that they are often interrelated. For instance, communication choices may need to be made when handling interruptions, or an interruption may need to be handled to deal with an urgent

[6] "Communication" refers not just to the contents of verbal or written conversations, but also to other more implicit interaction aspects, such as IM status, calendar entries, or code submission time stamps, which can serve to communicate awareness information about actions, availability, etc.

situation.

### 8.4.1 Making Communication Choices

Our interviewees indicated that privacy concerns impacted their communication choices, i.e., what was communicated to whom and how. Several privacy management practices occurred in the context of communication, such as self-censorship, medium switching, location switching, etc. When engaging in these practices, interviewees reported taking into account the situational characteristics outlined in our framework. Thus, the choice of privacy management actions depended on factors such as the importance, sensitivity, and confidentiality of the matter being communicated (*issues*), hierarchical as well as social relationships with the audience (*relationships*), temporal considerations such as whether or not the communication could be archived and accessed at future times (*temporality*), the richness of expression afforded by a communication technology (*technology*), and the presence of others around oneself who may come to know about the communication (*space*).

Commensurate with our framework (see Figure 8.2), the link between a particular communication situation and the corresponding privacy management actions is established by the interpretive influences. For instance, some individuals preferred IM over email for short messages (*self, issues*). Interviewees also reported that their communication choices were influenced by the norms in the team, and the management style of their manager. For example, some participants reported backchannel IM conversations with other team members in order to present a "uniform voice" during meetings with others, while others reported being available by mobile phone at all times because of managerial expectations (*team*). Site-specific influences were also observed: due to cubicle environments at some of the sites, private phone conversa-

tions necessitated reserving conference rooms or stepping outside the building (*site*). General organization-wide influences such as the shared technical infrastructure, and corresponding communication norms (e.g., on sharing one's calendar or accessing the calendars of other employees), also shaped how privacy was managed in communication (*organization*). Moreover, external factors unrelated to work, such as family, commuting conditions, and the cultural background, influenced how situations were interpreted (*cultural environment*).

Interviewees expressed vastly different expectations of privacy for written vs. non-written communication (*technology*). Written communication (which included email) was composed with care, and was often self-censored (*issues, relationships, self, organization*). The fact that it could be saved, or be forwarded beyond the original recipient, was often taken into account (*temporality*). The choices of whom to copy, or leave out, were made deliberately (*issue, relationships*). Interviewees also applied their interpretations to the variety of non-communicative functions of written communication, such as its role as an individual memory aid, knowledge management archive, organizational record, and instrument of accountability. On the other hand, non-written communication (such as phone calls and face-to-face meetings) was more informal and impromptu (*relationship, technology, team, site*). In terms of privacy, it was sometimes used for discussions deemed too sensitive for the written medium and/or when the individual wished to avoid a written trail (*issue, technology, temporality*). IM fell somewhere in between (Voida et al., 2002). Although IM is written communication, a majority of our interviewees treated it as ephemeral and informal. With the exception of a few, who exercised the same caution with IM as with email, the interviewees did not report archiving IMs (in fact, some even claimed not to know that it was possible to save IMs), and assumed that other employees did not save IMs either (*technology, temporality, organization*).

### 8.4.2 Handling Interruptions

One characterization of privacy is "freedom to be left alone" (Warren and Brandeis, 1890), i.e. control over access to oneself. Interruptions, which are common in knowledge work (González and Mark, 2004), have a direct impact in this regard (Altman, 1975). Our interviewees mentioned several kinds of interruptions, planned as well as unplanned. These included: scheduled meetings (*temporality*), incoming communication (e.g., email, IM, phone) (*technology*), colleagues dropping by one's office (*relationships*), urgent issues that required immediate attention (*issues, temporality*), and lunch breaks (*temporality*). We noted several privacy management practices for dealing with interruptions: closing the office door (*space*), scheduling "busy" blocks on one's calendar (*temporality, technology*), turning off IM or setting the IM status to "busy" (*technology*), multitasking during conference calls (*temporality, technology*), eating lunch at one's desk (*temporality, space*), working from home (*space*), and working during hours when few others are present (*temporality*).

Interruptions exhibited disruptive as well as useful characteristics. On the one hand, interviewees complained that interruptions took attention away from their current tasks (*issues*), required extra time and effort for refocusing on the original task (*issues, temporality*), and split time into short blocks resulting in the "filler" blocks being spent unproductively (*temporality*). On the other hand, interviewees recognized the value of interruptions learning about issues that required immediate attention (*issues*), coordinating with colleagues (*issues, relationships, temporality*), taking a break (*temporality*), multi-tasking (*issues, temporality*), interacting with friends and colleagues at the workplace (regarding work as well as non-work matters) (*relationships*), and attending to domestic errands (*issues, space*).

In handling interruptions, privacy management involved applying the interpretive

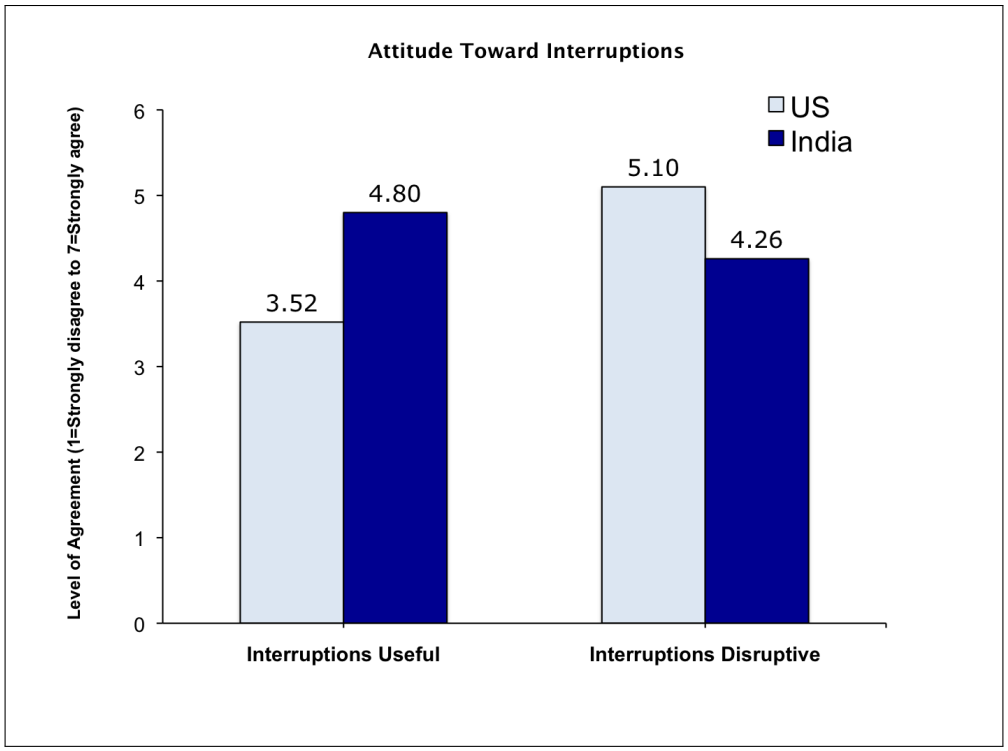


Figure 8.3: Contrasting attitudes towards interruptions at the U.S. and India sites

influences to resolve the tension between the disruptive influences of interruptions with their potential usefulness. (Note that merely "mentally processing" an interruption is also disruptive even if the interruption is not dealt with immediately.) For instance, we found that the job function affected preferences regarding how the tension ought to be resolved (*self*). For example, managers recognized greater value in interruptions since managerial duties require them to be available to resolve the issues brought forth by their subordinates (Hudson, James M. and Christensen, Jim and Kellogg, Wendy A. and Erickson, Thomas, 2002). In contrast, developers desired long, uninterrupted time blocks to concentrate on their programming tasks. Based on responses to the online questionnaire, we also uncovered differences between those at the U.S. sites with those in India (*space, site, cultural environment*) (see Section 8.6). As Figure 8.3 shows, those in India agreed more than those in the U.S. that interruptions are useful (India: 4.80, US: 3.52, $p < 0.0001$). In contrast, workers at the U.S. sites found interruptions disruptive to a larger extent (India: 4.26 US: 5.10 $p < 0.015$).

### 8.4.3 Balancing Work and Home

As mentioned in Section 8.2, it was not uncommon for Project X members to work from home, at least in the U.S.[7] (*organization*). The form of telecommuting ranged from occasionally checking email from home to having a permanent home office (*temporality, space*). Most of our interviewees fell somewhere between these two extremes (see Section 8.2). Moreover, more than half of our interviewees worked from home during late evenings and/or early mornings (*temporality*). This was necessitated by the need to "get work done" in long uninterrupted time blocks (*issues, temporality*), to "catch up" with unfinished tasks (*issues, temporality*), to handle urgent matters (*issues, temporality*), to interact with people in other time zones (*issues, relationships, temporality, technology*), and to build new knowledge and skills. Similarly, several interviewees admitted attending to domestic tasks at the workplace (*issues, temporality, space*). Examples include errands, doctor's appointments, personal email/IM/Web activities, family phone calls, or childcare tasks[8]. Traditionally, the two primary spheres of an individual's life – domestic and professional – have been markedly distinct. For Project X workers, however, the possibilities of getting work done even when away from the office blurred the boundary between home and work, and consequently impacted the traditional notion of the 9-to-5 work day (*temporality, space*). A second factor impacting the notion was the time zone differences with one's collaborators (*temporality*). As a result, what was considered to be "typical" work hours varied from location to location (*site*) and person to person (*self*).

Privacy expectations at home and at work are different. Accordingly, we noted several privacy management practices to balance work and home based on one's interpreta-

[7]Telecommuting was practically non-existent in India due to the lack of adequate domestic technical infrastructure, and demographic and cultural differences (*cultural environment*).

[8]Interestingly, the India site employed a person who was charged solely with attending to the domestic errands of the knowledge workers (e.g., paying bills at different places in town) *cultural environment*.

tion of the telecommuting situation. Outside of the standard business hours, almost all interviewees desired and exercised more control over their availability to others (*issues, relationships*) and over the tasks they worked on (*issues*). For example, during non-business hours some interviewees chose not to sign-in to IM (*technology*), or chose to work on tasks that did not require interaction with others (*issues*). In many cases, such preferences (*self*) applied regardless of one's physical location during these times, i.e., regardless of whether one was working at home or from one's workplace (*space*). For instance, frequent telecommuters reported that during standard business hours, they strived to make themselves available to their collaborators to the same extent that they would at the workplace (*temporality, space, team*). Most interviewees also reported designating a separate room or work space at home (*space*), and trying to separate work and home activities by using separate computers and phones (*issues, technology*).

### 8.4.4 Dealing with Urgent Matters

While all the situations discussed above pertain to normal routines, dealing with urgent matters (*issues, temporality*) required deviating from typical privacy expectations and practices. Judgments of urgency were based not only on the matter at hand but also on the parties involved (*relationships*). For instance, a request from one's boss was often assigned higher urgency. Discussions of urgency came up frequently in our interviews; participants stated that "normal" privacy expectations and practices did not apply in urgent situations. In such cases, they engaged in privacy management practices different from their normal preferences (*self*): reorganizing their calendar to devote time to "put out the fire" (*issues, temporality*), limiting their availability for other tasks (*issues, temporality*), making themselves reachable on their mobile phones (*temporality, space, technology*), answering phone calls at odd

hours (*temporality, space, technology*), and ensuring their availability even on vacation (*temporality, space*). Others were expected to make similar adjustments to their privacy expectations. Thus, when urgent matters arose, our interviewees interrupted others (*issues*), preferred a phone call over an email (*issues, technology, temporality*), called the mobile phones of their collaborators (*issues, technology, temporality*), or contacted higher-level managers with whom they would not normally communicate (*issues, relationships*).

In general, the views of all stakeholders (*team, site, organization*) on what should be regarded as urgent were aligned, but not always. The interviewees reported a handful of instances of differing interpretations of urgency. Since urgency led to changed privacy expectations and practices, mismatches in urgency evaluations could pose problems (such as receiving a phone call in the middle of the night for an issue that one does not deem equally urgent as the caller).

## 8.5 Impression Management

As can be expected based on our impression management model (see Figure 6.1), many of the responses of our interviewees reflect a desire for impression management. For instance, the following quotes taken from the interviews show the desire to convey an appropriate (e.g., "professional") impression and to manage the conveyed impression based upon the expected audience:

- *"I'm typically very professional in the way I craft my emails."* - Darren (Architect)
- *"When I write emails or IMs I have a certain expectation of who the target audience is. I have an expectation that the communication is not going beyond*

*the people that are part of it. I may say things in a different way depending upon the audience."* - Mark (Tester)

- *"My personal calendar is mixed with the work calendar. If the details were exposed to everyone, I would put things in differently. It's a bunch of men here - engineers - if I worked in an environment where there were more women, it might be different. I am concerned about how it's going to be perceived."* - Liz (Manager)

- *"I am worried about being perceived as a late responder by remote collaborators."* - Oliver (Manager)

- *"With people I don't know so well, I am reluctant to expose any lack of knowledge. I don't want to sound like an idiot."* - Steve (Developer)

- *"People would remember that you missed the deadline but ignore that it was due to quality considerations."*- Paul (Developer)

- *"I very rarely do any personal stuff from the work computer out of fear that someone might look at it and have a feeling of impropriety."* - Peter (Manager)

- *"I am careful about what I write. I try to be very clear and tend not to strategize. I would call when I am concerned that email isn't private enough. I assume that with most email someone's gonna hold it up as I said do this or do it this way."* - James (Architect)

Project X members also indicated a desire for the visibility of their conveyed impression with 83% of the questionnaire respondents indicating agreement with the statement "I would like to know how others perceive me based on my interactions with them" at a level greater than 5 on a 1-7 scale (see Figure 8.4).

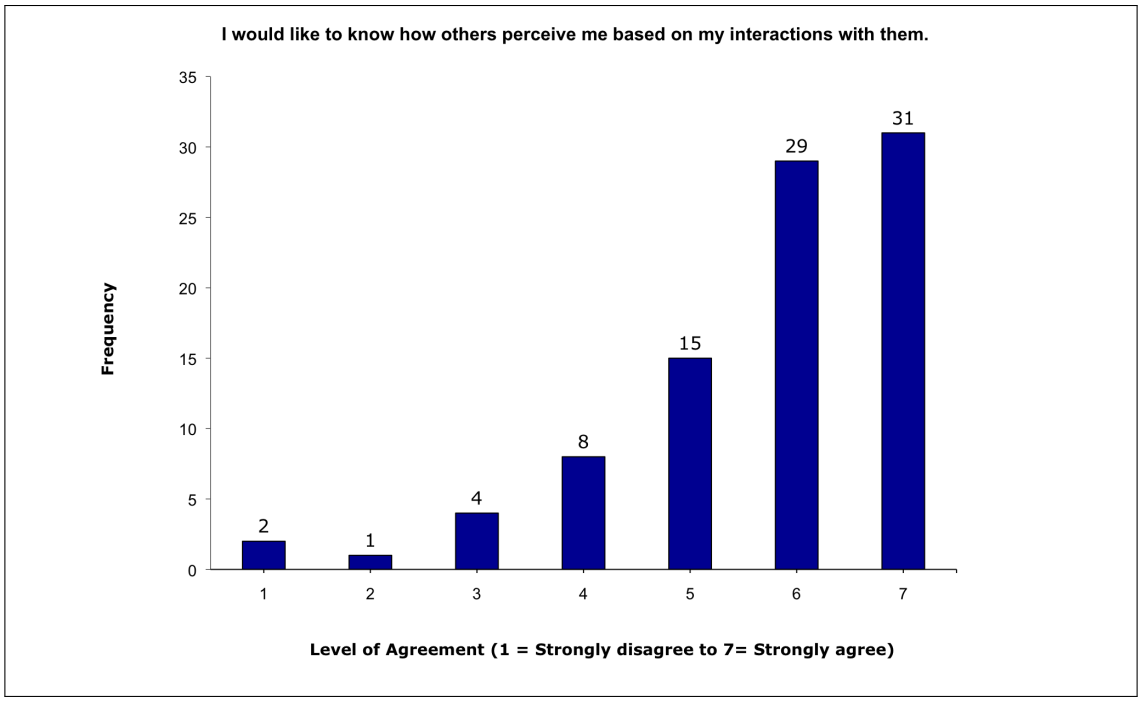


Figure 8.4: Desire for visibility of how one is perceived based on one's interactions with others

These impression management considerations often influenced the choice and prioritization of the situational characteristics and the interpretive influences described in our privacy management framework (see Section 8.3).

## 8.6 Comparison between the U.S. and India

Prior work that looked at online privacy in India found that Indians express lower privacy concerns compared with those from the U.S. For instance, Kumaraguru et al. (2005) report "an overall lack of awareness of privacy issues and less concern about privacy in India than has been found in similar studies conducted in the United States." Similarly, Cho et al. (2009) found that privacy concerns were the highest in New York and the lowest in Bangalore. Further, they discovered that Hofstede's (Hofstede, 2001, 2004) dimension of Individualism was one of the statistically significant

predictors of privacy concern with users from countries with a high Individualism score exhibiting higher levels of concern about online privacy. The U.S. has a high Individualism score of 91 (compared with the world average of 43), whereas India scores only 48. In our own field work (see the section on methodology), we noted the crowded and densely-packed nature of Indian work as well as life context leading us to suspect that higher collectivism (Hofstede, 2001, 2004) coupled with the necessity and experience of having others in close proximity would result in Indians harboring lower expectations for privacy. Therefore, we formulated the following hypothesis:
**H:** *In the context of workplace collaboration, knowledge workers from India would express lower privacy concerns compared with those expressed by their colleagues in the U.S.*

In order to compare attitudes across the U.S. and India, we divided the questionnaire respondents into two groups: those who worked at the India site (India) and those who worked at any U.S. site (US). Group US consisted of individuals of various nationalities (including some Indian citizens). Since context external to work can affect privacy considerations (Milberg et al., 1995; INRA, 1997; IBM, 1999; Zhang et al., 2002; Bellman et al., 2004; Ipsos Reid, 2006), we excluded from Group US those who had not lived in the U.S. for at least five years. (Prior research suggests that five years is a reasonable length of time to assume acclimatization to a different external context (Khan and Khan, 2007).) Even though Group India consisted wholly of Indian nationals, for the same reason, we excluded from Group India those who had lived in the U.S. for longer than five years before returning to India. The final dataset after the filtering comprised of 52 individuals in Group US and 35 in Group India.

True to the expectations of lower privacy concerns in India, we found that Group US reported significantly higher engagement in practices regarding protecting the privacy

of personal information from third parties (all differences are statistically significant at the 0.01 level). Specifically, these practices (which were taken from prior surveys from the domain of consumer privacy (IBM, 1999; Westin, 1991)) include: inquiring about organizational policies regarding personal information, refusing to provide personal information or refusing to make purchases if the organization did not protect personal information adequately, asking to remove one's personal information or prohibiting the sale of one's personal data, and checking to see which personal information about oneself had been collected by an organization.

To address our hypothesis, the questionnaire also asked respondents to rate how concerned they were about privacy with regard to various categories of people with whom they interact in the course of their work (on a 7-point scale from "completely unconcerned" to "extremely concerned"). These groups were: team members at the local site (excluding the manager), team members at remote sites (excluding the manager), manager, Project X peers outside of one's team at the local site, Project X peers outside of one's team at remote sites, upper management, company employees at the local site (but not working on Project X), company employees at remote sites (but not working on Project X), subordinates (if applicable), and system and IT administrators and support staff. In this case, however, we were surprised to find that, contrary to our hypothesis, individuals in Group India expressed higher privacy concerns than those in Group US. Pairwise t-tests for the differences are statistically significant for those categories of contacts that one would expect to work closely with viz., local and remote team members, manager, and local and remote Project X members. This can be seen in Figure 8.5 which plots reported privacy concerns of the two groups for each of the categories. Although the differences for the other categories are not statistically significant (see Table 8.2), the privacy concerns of Group India are still higher except in the case of subordinates.

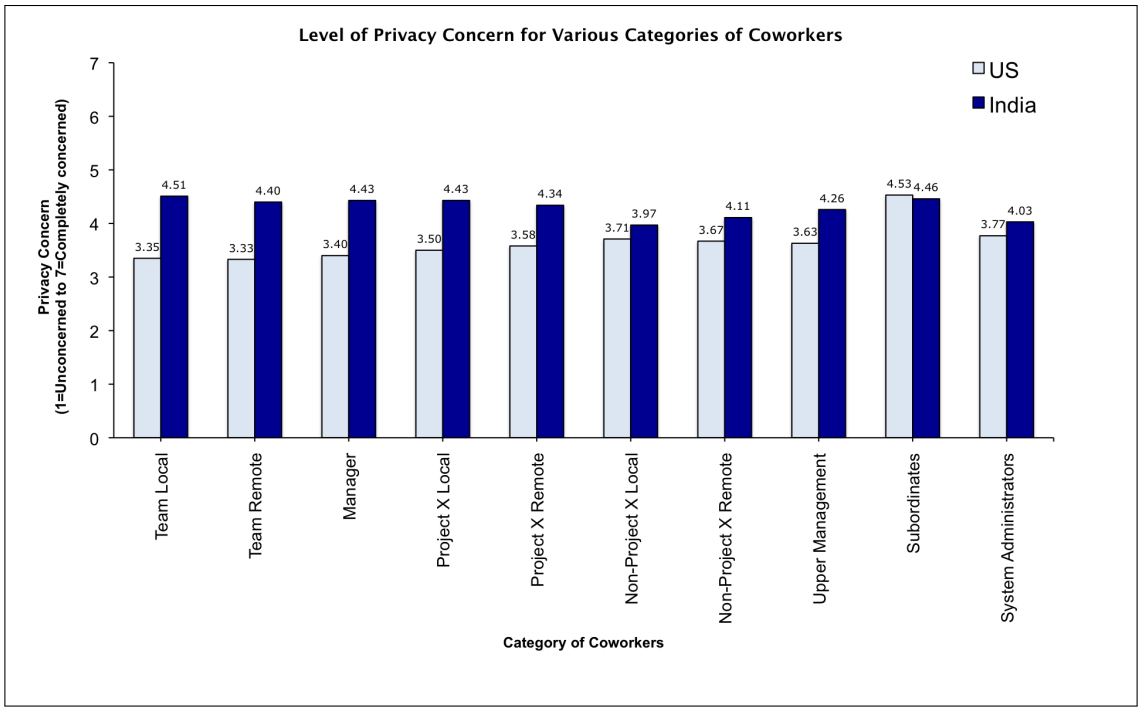


Figure 8.5: Average reported privacy concerns of Group US and Group India for various categories of people on a scale of 1 (completely unconcerned) to 7 (extremely concerned)

In a similar vein, on a scale of 1 (strongly disagree) to 7 (strongly agree), those from Group India express a higher desire for privacy management tools (India: 5.1 and US: 4.27, $p < 0.033$). Group India also indicates a slightly higher willingness to spend time in configuring such tools if they offer better privacy management (India: 4.9 and US: 4.5, $p < 0.27$) although this difference is not statistically significant.

Interestingly, we found that the interpersonal privacy concerns expressed by respondents in both Group India and Group US were affected by the extent to which the individuals were concerned in general about privacy on the Internet. To gauge the level of general privacy concern about online activities, we used a question borrowed from prior consumer privacy surveys (IBM, 1999; Westin, 1991): How concerned are you about threats to your personal privacy when you are online? The respondents could answer on a scale of 1 to 4 with 1=Very, 2=Somewhat, 3=Not very, and 4=Not at all. We pooled the respondents concerned at levels 1 or 2 as those with high online

Table 8.2: Levels of reported privacy concerns of Group US and Group India for various categories of people

| Group | N | | Mean | | Median | | Mode | | p |
|---|---|---|---|---|---|---|---|---|---|
| | US | India | US | India | US | India | US | India | |
| Team Local | 52 | 35 | 3.35 | 4.51 | 3 | 5 | 4 | 6 | 0.0043 |
| Team Remote | 52 | 35 | 3.33 | 4.40 | 4 | 4 | 4 | 4 | 0.0031 |
| Manager | 52 | 35 | 3.40 | 4.43 | 3 | 5 | 1 | 5 | 0.0092 |
| Project X Local | 52 | 35 | 3.50 | 4.43 | 4 | 5 | 4 | 5 | 0.0077 |
| Project X Remote | 52 | 35 | 3.58 | 4.34 | 4 | 4 | 4 | 4 | 0.0287 |
| Non-Project X Local | 52 | 35 | 3.71 | 3.97 | 4 | 4 | 4 | 4 | 0.4695 |
| Non-Project X Remote | 52 | 35 | 3.67 | 4.11 | 4 | 4 | 4 | 4 | 0.2117 |
| Upper Management | 52 | 35 | 3.63 | 4.26 | 4 | 4 | 4 | 4 | 0.4656 |
| Subordinates | 38 | 28 | 4.53 | 4.46 | 5 | 5 | 5 | 5 | 0.8878 |
| System Administrators | 52 | 35 | 3.77 | 4.03 | 4 | 4 | 4 | 4 | 0.4656 |

privacy concern and those concerned at levels 3 and 4 as those with low online privacy concerns. We also calculated a single level of interpersonal privacy concern for each respondent by averaging across the various groups listed in Table 8.2. As Figure 8.6 shows, both Group India and Group US show an increase in interpersonal privacy concern with an increase in concerns about online privacy. For Group US, the correlation between interpersonal and online privacy concerns is statistically significant at 0.01 level. For Group India, although the same trend is observed in Figure 8.6, the correlation is not statistically significant. We suspect that this is due to the relatively small number of respondents in Group India with high online privacy concerns. (As Table 8.3 shows only 30% of the respondents in Group India expressed high online privacy concerns as opposed to nearly 75% of those in Group US.)

The relative percentages of those with high and low online privacy in Group India and Group US are almost opposite of each other (see Table 8.3). Combining this

Table 8.3: Number of respondents in Group India and Group US split by level of online privacy concern

| Online Privacy Concern | US | India |
|---|---|---|
| High | 38 (73%) | 10 (30%) |
| Low | 14 (27%) | 25 (70%) |

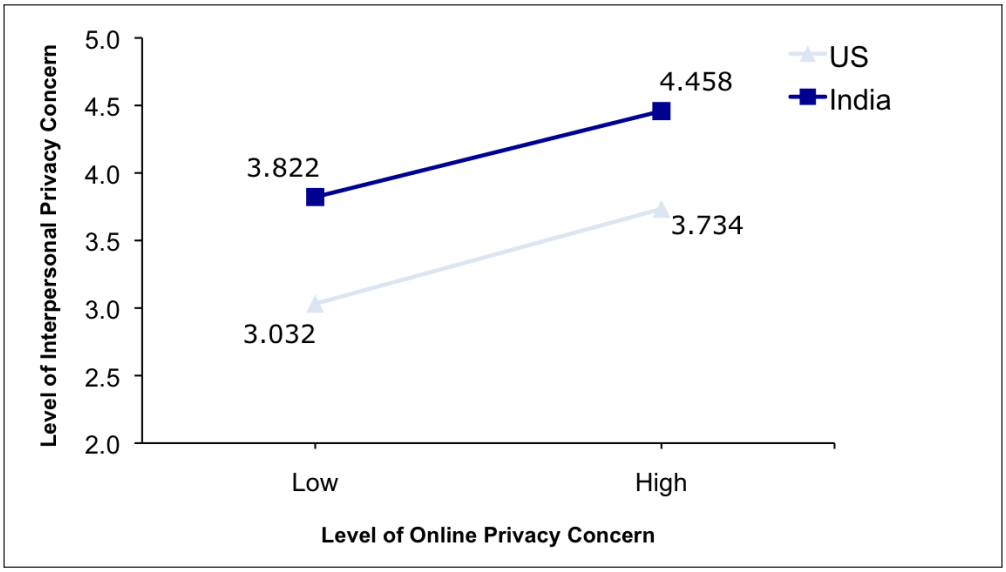


Figure 8.6: Interpersonal privacy concern by different levels of online privacy concern

observation with the relationship between online and interpersonal privacy concerns discussed above, we sought to refine the differences observed in Figure 8.5 by further splitting Group India and Group US into two subgroups: those with low and high online privacy concerns respectively. Figure 8.7 compares the magnitude of the difference in reported privacy concerns for the various categories among the subgroups with low and high online privacy concerns respectively.

It can be seen in Figure 8.7 that the differences are higher when those with low online privacy concerns from Group India are compared with those with similar (low) online privacy concerns from Group US. and lower when the two subgroups with high online privacy concerns are compared. This is noteworthy given that prior research (Kumaraguru et al., 2005; Cho et al., 2009) suggests that the relative percentages of those with low and high online privacy concerns in India and the U.S. populations may be

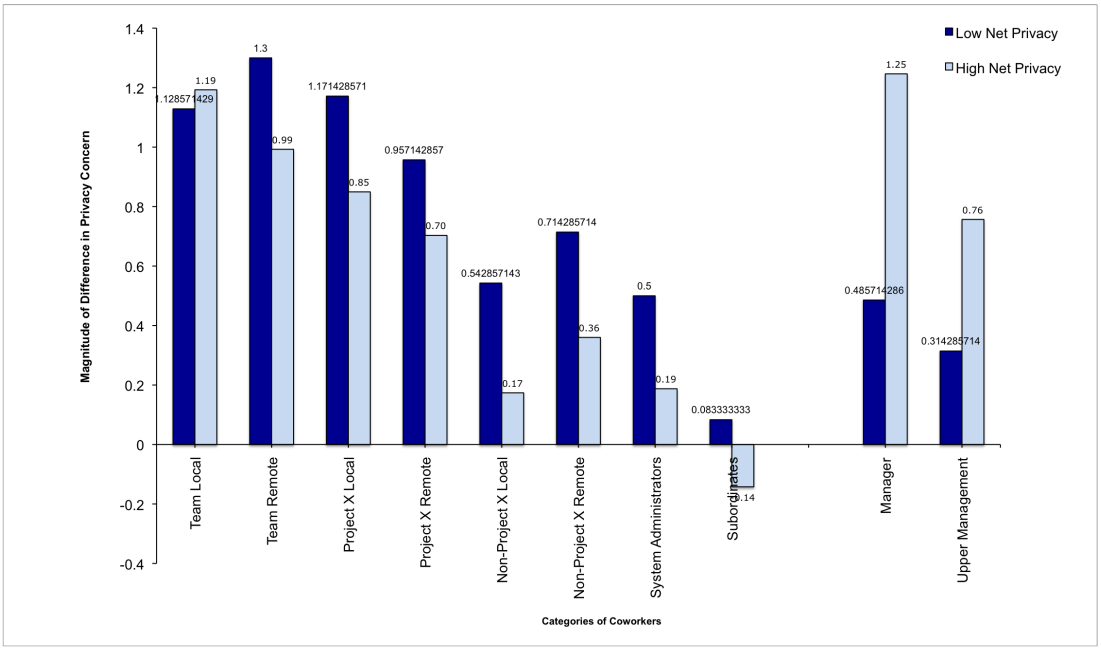


Figure 8.7: Comparing the magnitude of the difference in interpersonal privacy among subgroups expressing low and high online privacy concerns respectively

similar to those in our sample.

There are two notable exceptions: team members at local sites (as seen in Figure 8.7 at extreme left) and management (as seen in Figure 8.7 at extreme right). The former shows relatively little change across subgroups. This suggests that the social, collaborative and physical proximity with local team members may ameliorate the impacts of differences in online privacy concern. As far as management is concerned, the results of the comparison are opposite to that in the other cases. This could be due to differences in the management style and in attitudes towards management in India and the U.S. (see the discussion in the following section).

We also compared the reported attitude of the two groups towards interruptions, a factor linked frequently to privacy in the literature (Altman, 1975). As Figure 8.3 shows, despite expressing comparatively higher privacy concerns, Group India finds interruptions useful to a much larger extent than Group US on a scale of 1 to 7 (India:

4.80, US: 3.52, $p < 0.00001$). On the other hand, Group US, despite expressing comparatively lower privacy concerns finds interruptions disruptive to a much larger extent (India: 4.26 US: 5.10 $p < 0.015$).

## 8.7 Discussion

To uncover plausible explanations for the surprisingly higher privacy concerns of Group India, we delved deeper into the data from our questionnaire, interviews and field visits. Based on this analysis, we believe that one or more of the following factors account for the observed discrepancy:

### 8.7.1 Physical Characteristics of the Workplace

Prior research shows that the physical characteristics of the workplace play a role in employee attitudes and work practices. Stokols et al. (2002) found that environmental distraction was significantly linked to employee perceptions of support for creativity at work, which in turn affected job satisfaction and stress. Specifically regarding privacy, Sundstrom et al. (1982) discovered that privacy ratings of the workplace increase with increase in the number of partitions. Kupritz (1998) further analyzed the relationship between various design features of the physical work space to several possible work activities requiring various forms of privacy.

Our site visits had brought to our attention that the physical characteristics of the India site were substantially different from any of the U.S. sites (see Figure 8.1). As the top left picture in Figure 8.1 shows, the Indian site was arranged as a dense cubicle farm with dividers that barely rose higher than the sitting height of a person. The low height of the cubicle dividers caused individuals' computer screens to be

Table 8.4: Employee density at the Indian site compared with the sites in the U.S.

| | India | US |
|---|---|---|
| Employees | 621 | 2,319 |
| Area including common spaces (sq. feet) | 89,157 | 973,142 |
| Density (sq. feet / employee) | 144 | 419 |

visible to a large number of people at any given time. Moreover, the site in India was densely packed compared to those in the U.S. (see Table 8.4 for a comparison of the area and density of the India site compared to the average area and density across the sites in the U.S.). It was not uncommon for as many as five individuals to share a cubicle. Sometimes even managers were assigned to a cubicle shared with, or next to, those they supervised. Upper management did receive the privilege of a private cabin. However, these cabins were made of fully transparent glass. As a result, it was extremely difficult, if not impossible, to carry out any physical or digital action in seclusion.

In contrast, all employees at two of the three U.S. sites we visited occupied office rooms, either by themselves or shared with one other person. The middle picture on the right of Figure 8.1 shows a corridor of such offices with a view into an office. Employees at the third location occupied cubicles, again by themselves or shared with one other person. However, these cubicles were much larger (with dividers reaching almost up to the ceiling) than those at the Indian site and were equipped with doors. The top right picture in Figure 8.1 shows a view of these cubicles in contrast with those in India in the picture just to its left. The bottom right picture in Figure 8.1 highlights the presence of spacious, uncrowded common areas at the U.S. sites in contrast to the crowded nature of the India site.

Prior studies have confirmed the impact of "open-plan" offices on privacy. Haans et al. (2007) reported that Dutch bank employees working in such an office with little visual

and auditory separation between work spaces indicated a higher need for privacy compared with those working in a mixed office design. Additionally, "employees who had to share their desk with others had an even higher need for privacy in open-plan offices" (Haans et al., 2007). Birnholtz et al. (2007) offer insight regarding how workers in North American open-plan offices cope by lowering their privacy expectations and drawing upon shared understanding of "legitimate targets of attention" in the physical space. A literature review (De Croon et al., 2005) provides strong evidence that working in open workplaces reduces privacy and job satisfaction. There is also some evidence that open-plan and densely packed workplaces increase cognitive workload, decrease the quality of interpersonal interactions and reduce privacy (De Croon et al., 2005). Thus, we believe that the differences in workplace layout is one of the factors underlying the elevated privacy concerns expressed by Group India.

### 8.7.2 Nature of Interpersonal Relationships

Culturally, interpersonal relationships are known to play an important role in Indian society (Miller and Bersoff, 1999). As a result, Indians are likely to spend more time and effort in managing these relationships as compared to that for privacy-preserving actions in dealing with consumer data protection from impersonal third parties and organizations. We also found that on a scale of 1 to 7, Group India expressed a slightly greater desire than Group US to know how others perceive them based on their interpersonal interactions (India: 6.03, US: 5.44, $p < 0.05$). Section 6.2.1 showed that such desire for relationship-appropriate impression management is an antecedent of privacy concerns (Kobsa et al., 2010).

This is evident in Table 8.2 and Figure 8.5 which show larger, statistically significant differences in privacy concerns for those categories with closer working relationships

(viz., Team Local, Team Remote, Manager, Project X Local and Project X Remote). Subordinates seem to be an exception, perhaps because, as indicated in our interviews, managers wished to protect the privacy of their staff members from other employees, and also desired confidentiality of sensitive managerial communication from subordinates.

### 8.7.3 Conceptualization of Privacy

Since the conception of privacy of each of the respondents may not completely overlap with the others, it may also be the case that some of the differences between Group US and Group India stem from cultural differences that lead to only a partial overlap regarding what is encompassed by the concept of privacy (Kumaraguru et al., 2005). We already discussed the contrast between privacy concerns expressed in the daily work domain and privacy-preserving actions performed in the eCommerce domain. Consider, also, the issue of interruptions where the Western perspective suggests a positive correlation between higher levels of privacy with lower levels of interruptions. Yet, as mentioned above, the attitudes of Group India regarding usefulness and disruptiveness of interruptions run counter to their reported higher concerns about privacy. Based on these observations, we feel that some part of the differences in the reported privacy concerns could be attributed to the lack of complete alignment between the two groups regarding how privacy is conceptualized.

### 8.7.4 Intra-team Competition

In India, the job market for knowledge workers (particularly in IT) is extremely competitive. Individuals constantly seek better work prospects both within and outside the company. As a result, one is always competing with others for "credit" and "ex-

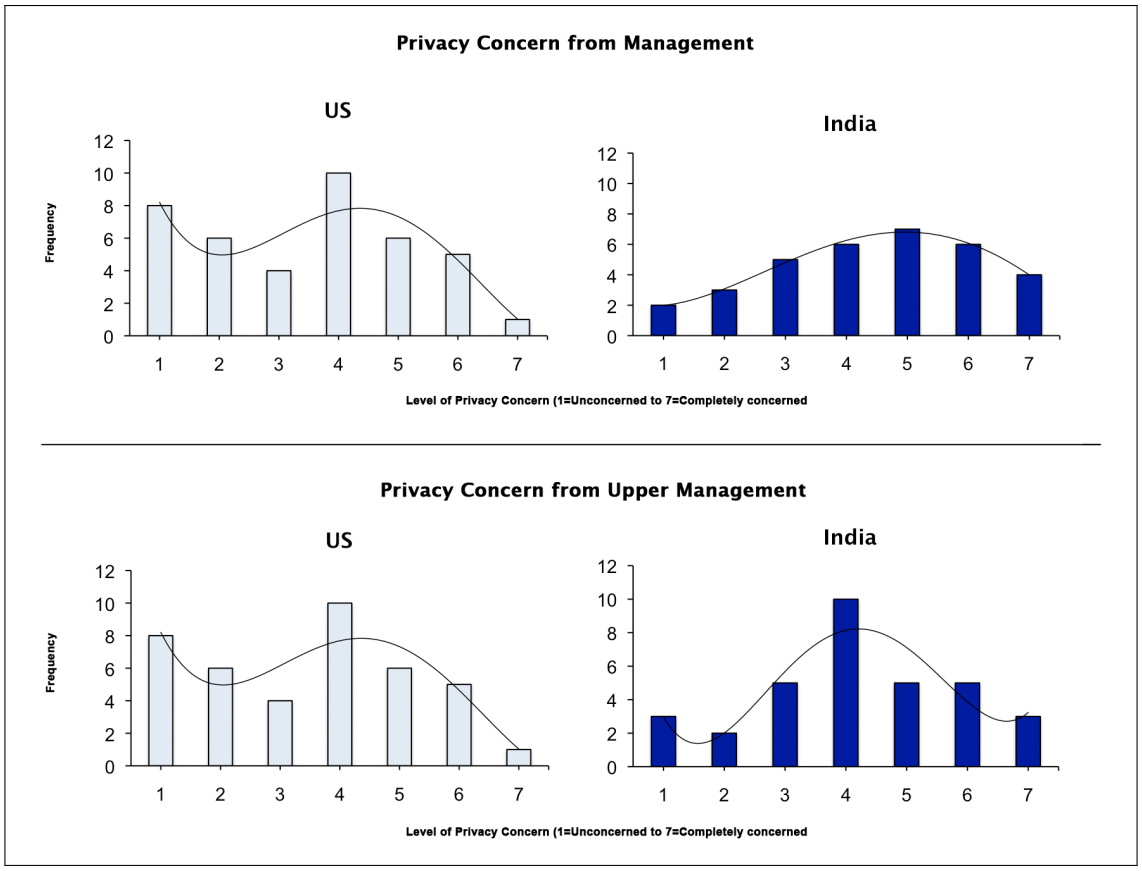


Figure 8.8: Privacy concerns from management

perience." Indeed, Group India rated the competition within their teams to be higher than Group US (India: 3.46, US: 3.00, $p < 0.03$). Competing with one's team would likely elevate the desire for privacy with respect to the team members.

### 8.7.5 Management Style and Hierarchy

The findings section hinted that privacy concerns in relation to management may be somewhat different as compared to those regarding other colleagues. Additionally, during our field visits and interviews, we observed that the style of management at the India site appeared to differ in comparison with the sites in the U.S. For instance, individuals in India required more managerial "hand holding," both in terms of coaching and in terms of handling matters requiring decision-making authority.

Moreover, communication with off-site individuals was frequently channeled through management. In contrast, those at the U.S. sites reported working more independently and exercising greater discretion and autonomy in making decisions regarding less important matters.

Prior research also points to differences between India and the U.S. in terms of hierarchical relationships. Specifically, Hofstede's cultural dimension of Power Distance is a measure of "the extent to which the less powerful members of organizations and institutions (like the family) accept and expect that power is distributed unequally" (Hofstede, 2001, 2004). Compared with the World average value of 55, the Power Distance Index for India is much higher (77) whereas that for the U.S. is on the low end of the spectrum (40). Higher values of power distance are associated with greater inequality in power relations such as those between management and the managed staff. Indeed, literature on Indian organizations shows that superior-subordinate relationships are hierarchical, with an emphasis on superior guidance and subordinate loyalty and compliance (Khandwalla, 1988; Mathur et al., 1996; Parikh and Garg, 1990; Sinha, 1982, 1990). Similarly, Aycan et al. (1999) found that Indian managers scored high on paternalism, power distance and uncertainty avoidance. This results in "a dependent relationship between superiors and subordinates in which managers tend to assume lower employee proactivity and, consequently, do not promote employee autonomy on the job" (Aycan et al., 1999). Also assumptions of employees reactivity leads managers to set specific goals and to plan in detail because they believe that employees need direction and close supervision.

We, therefore, took a closer look at the privacy concerns of Group India and Group US in relation to their managers as well as upper management. We filtered out the responses from managers from both groups, leaving us with 33 non-managerial respondents for Group India and 40 for Group US. We then plotted the frequency

distributions of these groups for the level of privacy concern regarding their managers and upper management (see Figure 8.8). Figure 8.8 shows that Group US is slightly skewed towards the lower end while Group India is slightly skewed towards the higher. More interestingly, Group US shows greater variance in the answers. This suggests greater alignment of attitudes towards management among the subordinates from Group India, in line with expectations of subordinate acknowledgement of hierarchical power relations associated with a higher Power Distance Index.

## 8.8 Methodological Insights

As the above discussion shows, the study was successful in shedding light on our research objective of discovering practices surrounding privacy and awareness issues. Concurrently, we also gained a number of methodological insights from the discussions among the research team regarding the choice of appropriate methodology to study collaboration in globally distributed software teams, and from the experiences gained when using our methods in practices.

Some of these discussions centered around aspects that are common to all studies that utilize a particular method, e.g., how to avoid leading questions in an interview, or select appropriate scales in a survey. Each method has its own extensive body of research regarding its strengths, weaknesses and applicability, discussed in several textbooks and publications (see e.g., (Hammersley and Atkinson, 2007; Fowler, 2008; Kvale and Brinkmann, 2008)). We will therefore not discuss them further, but focus instead on the distinguishing characteristics and factors of the globally distributed software project that impacted our methodological choices. Given that most of these aspects appear to be common to all globally distributed software engineering efforts, we believe that these discoveries can serve as a useful resource when designing and

conducting empirical studies of global software teams.

### 8.8.1 Access

Our first challenge was to gain access to the project. We talked with top management (including the head of Project X) in order to "pitch" the study. In exchange for access, we had to promise a report with recommendations for improving the effectiveness and efficiency of the project. This top-level clearance was however not enough to grant us access to each of the five sites. We found that the following other factors were equally instrumental in eventually obtaining access:

#### Incentives

Although the mandate from the top was beneficial in gaining access, aligning the incentives of the organization, the management, the project members, and the researchers posed hurdles. For instance, a few individuals viewed participation in the study as a low-priority chore and were reluctant to devote time to it (e.g., one participant stopped the interview halfway and never scheduled a time to finish it despite repeated reminders). Similarly, we discovered that one manager was not overly thrilled with the upper management's decision that Project X participate in the study because it required his team to devote time to the interviews instead of "getting work done." This underscores the importance of not only securing buy-in from the top echelons, but also communicating to each project site and each project member the value provided by the research for the individual site, the project under study, and the organization as a whole.

### Affliation

Although the study was carried out as a collaboration between the corporation and a university, one of the research team members was employed full-time at the corporation as a summer intern during the first phase of the study (i.e., the non-participant observation, site visits and interviews). Subsequently, he was employed as an affiliate during the administration of the survey and the analysis of the study data. Being an organizational "insider" was critical for access; many of the study participants would probably not have devoted the same time and attention for an external researcher. Moreover, we noticed that interview participants took the organizational affiliation into account when divulging information deemed sensitive or confidential to the corporation. At the same time, we ensured that the interviewer did not know the informants. This was greatly helped by the fact that the interviewer was a summer intern and was therefore new and unknown to the other employees. This unfamiliarity was helpful in ameliorating discomfort in discussing sensitive issues. Thus, individuals who can bridge the different research entities are valuable for successfully conducting research projects that involve multiple organizations.

### Project Phase

As discussed in Section 8.2, the phase of the project impacted the amount and nature of work and consequently the levels of stress that the project members experienced. Therefore, we needed to schedule time with the project members during periods in which they were not racing against project deadlines. Knowing the temporal rhythms of the workflow was useful in maximizing participation and carrying out the research methods. We discovered these rhythms partly via our observations of the managerial meetings (see Section 8.1.1) and partly via direct communication with the

participants.

#### Vacations

Another factor that impacted participant availability besides the project phase was holidays and vacations. This issue is exacerbated in a global team because one needs to consider local holidays and typical vacation periods in each of the countries across which the collaboration takes place. For instance, we needed to reschedule our visit to India as initially planned because it was pointed out to us that the dates coincided with a two-week festival during which many employees were on vacation. Similarly, we were unable to interview a few of the participants in the U.S. because our site visits happened to coincide with their summer vacations.

### 8.8.2 Costs

A major factor that drives methodological choices is the cost of envisaged research methods in relation to the value of their results. In order to justify the research and gain access to the sites and project members (see Section 8.8.1), the anticipated organizational benefit must be higher than the cost of the research. Therefore, our research team needed to be cognizant of the total costs. In addition to expenditures that apply to any empirical study (such as researchers' time for conducting the study, analyzing the data, and reporting the results), there are two other types of costs that have a significant impact when studying globally distributed software projects:

**Travel costs:** Due to the high costs of travel to the remote sites, we could only visit them once for a week each. This, in turn, limited flexibility. For instance, as mentioned above, we could not interview those who were on vacation during

the period of our visit. Similarly, we could not observe the impact on work practices of local factors such as snow (which impacts the mid-U.S. site) or monsoon (which impacts the India site). In contrast, at the U.S. East Coast site at which we were based, there was considerably more leeway in scheduling or re-scheduling interview times as well as conducting follow-ups, if needed.

**Opportunity costs:** Knowledge workers in software projects earn high salaries. Since participation in the study was not part of their performance appraisal, the opportunity costs of participation are quite high for the project members as well as for the corporation. In addition to the salary rate, another factor that impacts these costs is attitudes and perceptions regarding "business hours." All our interviews and observations were conducted during business hours (9 am to 5 pm local time). For those who used these hours for critical work, the opportunity costs were quite high. On the other hand, the opportunity costs were lower for those who scheduled critical work during evenings and weekends (since during these periods they could work for long periods without interruptions (Patil et al., 2009)).

### 8.8.3 Cultural Sensitivity and Linguistic Issues

In order to study collaborations that span multiple countries, researchers must be able to discern the impact of cultural and linguistic differences. This can be achieved in two contrasting ways:

- Individuals with little familiarity with the country or the culture may be able to make observations that could otherwise be treated as mundane, unimportant or uninteresting. For example, we were able to spot the presence of deities and other religious symbols on the cubicle walls and computer screens at the Indian

site[9]. This practice might easily have escaped attention as not being noteworthy due to its commonality and taken-for-grantedness in Indian workplaces and society.

- Individuals with familiarity and experience with the country or the culture could formulate explanations for the findings by relating the data to the cultural context and social practices. For example, we were able to relate the interview and survey responses of our participants to local factors such as family life and expectations, commuting and traffic situations, job market conditions, technical infrastructure available at home, etc. (Patil et al., 2009).

In our case, the research team member who conducted all interviews and field observations at the India site, was born and raised in India. However, he had been living in the U.S. for the past several years. As a result, he could serve in both of the above capacities for the U.S. and also for India. The same was true for another member of the research team who had also grown up in India prior to moving to the U.S. The other members were American and European. This cultural diversity was extremely useful for us to be able to fill both of the above roles for the Indian as well as the American sites.

Despite this diversity, we needed additional clarification from "cultural insiders" in order to understand the surprising finding from our survey data, viz., employees at the India site exhibited higher privacy concerns compared with their colleagues from the U.S. (see Section 8.6). In order to validate and refine our explanations as well as discover new ones, we consulted with two independent parties: an Indian knowledge worker from the India site who was external to Project X, and an Indian knowledge worker from another Indian firm who had previously worked for a company in the U.S.

[9]This is particularly noteworthy because India is a constitutionally secular country.

Besides cultural peculiarities, language may also play an important role in research on global collaborative projects. In many non-English-speaking countries, for instance, the day-to-day affairs are conducted in the local language with English being used only when necessary for cross-national communication and for business matters. Moreover, non-native speakers of English often find it easier to express themselves in their native language. As a result, research methods employed at such sites ought to use the local language to the extent possible. Fortunately, language was not a major issue in our case since English is an official language in India, and widely understood and used among Indian knowledge workers. The interviews and the survey at the India site were conducted in English. However, we did note during the interviews that the English proficiency of many individuals at the India site was lower than that of their counterparts in the U.S. (regardless of whether those in the U.S. were native or non-native English speakers). It is possible that this difference in English proficiency impacted their understanding of the interview and survey questions, especially when dealing with an intricate concept like privacy.

We therefore suggest forming research *teams* with representatives from each culture and by conducting research in local languages to the extent possible. Achieving this, however, increases the costs of the research (see Section 8.8.2) and must therefore be balanced with the expected benefits.

### 8.8.4 Dynamics of Software Engineering

Various types of organizational dynamics that are particularly salient in fast-moving sectors like software engineering need to be taken into account when making methodological decisions:

**Organizational restructuring and business changes:** For strategic reasons, organizations restructure their workforce and/or projects, resulting in new work division across sites and changed work assignments for individuals. Teams may join or leave projects. For instance, just before our study began, teams from European sites had transitioned out of Project X.

**Employee turnover:** Employees may be laid off by the organization, or may leave of their own accord. Similarly, new employees may join. For example, during the course of our study, some employees quit working for the corporation. As mentioned in Section 8.1.4, we could not therefore obtain survey responses from all those whom we had interviewed earlier.

**Level of project involvement:** As discussed in Section 8.2.3, an individual's involvement in the project can vary from a small percentage of their work hours to full-time. Moreover, the level of involvement may be dependent on the phase of the project cycle.

These factors keep software projects in constant flux and can make it difficult to gather a stable picture of their characteristics, including team membership, roles, relationships among individuals, etc. For instance, the number of Project X members at the India site almost tripled during the course of our study. Therefore, it is important that the methodology not just capture a global software project at a given point in time, but also track its evolution due to corporate dynamics. In our experience, a detailed understanding of the project emerges only over a longer term (ranging from a few weeks to a few months). Given the dynamic nature of these projects, one methodological challenge researchers face is to accommodate potential changes in the project that may occur over the study duration.

### 8.8.5 Methodological Breadth

As described in Section 8.1, we applied a range of methods over a period of time to study Project X. This methodological breadth provided several advantages:

- The application of multiple methods allowed us to leverage their different strengths. For example, the conversational form of semi-structured interviews enabled us to probe deeper with follow-up questions and clarifications. On the other hand, the anonymity of survey responses allowed us to ask sensitive questions (e.g., items of the self-monitoring scale (Snyder, 1974)[10]) that may not have been answered candidly in a face-to-face conversation[11].

- The detailed description of Project X in Section 8.2 was not obtained directly in such a cohesive form. It emerged gradually over the course of the study by combining data obtained from the various methods.

- The data collected with some methods was useful in understanding and explaining the findings from others. For instance, had we not conducted in-person site visits, several important site-specific differences might have gone unnoticed. The meaning of the term "cubicle," for example, was completely different at the mid-U.S. site as opposed to the India site due to local differences such as the height of cubicle dividers, the number of people per cubicle, the area of the cubicle etc. (The left half of Figure 8.1 shows the cubicles at the India site while the picture at the top right shows cubicles with doors at the mid-U.S. site.) We were able to explain the differences between privacy concerns reported in India and the U.S. with these observations regarding the layout and physical features

[10]Notably, one of the project members emailed us that she was offended by these questions and refused to finish the survey.

[11]Some questions were deemed too sensitive even to include in the survey. For example, as per the organizational culture, income information was treated as highly personal and confidential and could not be asked for.

of the work places at the respective sites (see Section 8.7.1).

- To avoid bias, our methodology was designed to study collaborative practices in general (see Section 8.1). Understanding the broader collaborative context allowed a deeper analysis of the relationship between privacy and awareness expectations and practices, our research question in a stricter sense. For example, the interviews revealed close camaraderie between the software developers at the U.S. West Coast site which had developed due to having worked together for several years. This history had a great impact on their expectations of awareness of, and privacy from, each other. Similarly, the visit to the mid-U.S. site uncovered that the lack of an on-site lunch cafeteria had a negative effect on awareness.

These observations suggest that studies of complex global collaborations such as corporate software projects can benefit from application of multiple methods and from paying attention to routine work practices regardless of whether those practices are directly relevant to the research questions.

### 8.8.6 Data Sharing and Ownership

Since part of the research team was from a university, a research agreement needed to be worked out between the corporation and the university to cover issues such as access to study participants, and the ownership and sharing of data and intellectual property. This required acquiring approval from the office that oversees human subject research at the university as well as the legal offices of both organizations. This process was tedious and time-consuming, and no data could be collected or analyzed until a legal agreement had been worked out. Although not directly relevant to the study design, the delays and compromises required in drafting these collaborative

agreements may limit when and how some of the methods can be used. These issues could become even more difficult to work out if the entities involved in the research (researchers as well as the study settings) fall under different national jurisdictions, which may be the case when studying teams that are distributed across the world. Thus, research teams spanning multiple organizations must budget for potential delays and compromises regarding the research methodology and data sharing.

### 8.8.7 Alternate Methods

Practical considerations, such as access (see Section 8.8.1) and costs (see Section 8.8.2), prevented us from exploring alternate methods which might have provided substitutes or compliments to the methods we discussed in Section 8.1. Specifically, we could have derived additional benefit from the following methods:

**Participant observation:** An individual who worked on Project X could have served as an observer of the project, to validate and refine our observations based on first-hand experience.

**Analysis of project deliverables:** Computational analysis of the various deliverables produced by the project, such as requirement specifications, code, bug fixes, documentation, managerial reports, project plans, etc., could have revealed patterns not easily discernible otherwise.

**Shadowing:** Apart from attending management meetings (see Section 8.1.1), we did not observe people while they were engaged in their work on Project X. In-situ observation, especially when coupled logs of computing activities, might have helped uncover discrepancies between participants' responses and their actual behaviors. Shadowing would also have been helpful to study telecommuting

practices.[12]

**Focus group:** The results of a collective discussion of a focus group composed of Project X members could have complemented the individual perspectives we received from the survey and interview responses.

### 8.8.8 Implications

The discussion above holds several implications for designing future studies of globally distributed software engineering projects.

Firstly, despite the availability and use of technologies to bridge distances, the geographical distribution will always remain an important factor in such collaborations (Olson and Olson, 2000). Therefore, when making methodological choices, it must be kept in mind that globally distributed teams will differ from co-located teams. For instance, shadowing, which is often useful when studying co-located collaborative practices, may not be as effective when studying distributed collaboration because a majority of the collaborative activities are computer-mediated and cannot be observed directly. Instead, it might be more illuminating to study the outputs produced by the project and/or usage logs of computers or collaborative tools.

Secondly, as should be evident from Section 8.2, corporate software engineering projects are complex; they involve multiple job functions, processes, phases, and tools. Adding geographical distribution to the mix further increases their complexity. Investigating any research question requires that the methodology uncover the multiple connections between the various pieces of the project. These connections are the glue that holds the project together and enables its day-to-day practices. A narrower

[12]We decided against shadowing since it might have made the participants concerned about employer surveillance. Moreover, shadowing would have been possible only at the work places because it was impractical to gain access to people's homes to observe telecommuting.

focus risks overlooking important details. For instance, if we had limited ourselves to studying the developers and testers only, we might not have discovered how management bridges their routines with the larger goals and operations of the project. On a related note, as mentioned in Section 8.8.5, we found that an understanding of typical work practices not just helps avoid bias but also proves illuminating regardless of the specific research question.

Thirdly, as discussed in Section 8.8.4 the methodology ought to take into account the dynamism and evolution inherent in software engineering projects. This may require that studies be conducted over a sufficiently long period of time, or that they be repeated at appropriate intervals. Methodology should also be flexible enough to accommodate changes in the project that occur over the duration of the study.

Fourthly, our experience illustrates the leverage and benefits that can be achieved by using multiple methods to unpack the intricacies of a project (see Section 8.8.5). Not only did the methods provide different strengths and findings, but they also facilitated the discovery of relationships between the findings. For instance, our initial inclination was to conduct phone interviews with project members at remote sites without an actual visit to the site. However, the addition of site visits allowed us to uncover the important role played by the local site architecture and physical features in shaping collaborative work practices and expectations. As Section 8.8.5 points out, this understanding also helped us explain our findings.

On a more practical note, we also want to point out the opportunities for building better tools that make it easier to conduct such studies and to analyze the collected data. We utilized a plethora of tools for taking field notes, recording the interviews, transcribing the recordings, analyzing the transcripts, creating and deploying the survey, and analyzing the survey responses. In addition, we also needed to manage the planning and scheduling aspects of dealing with the participants. While each of

the tools was effective for its specific purpose, it was often cumbersome to integrate the data and information and to move between the tools. For example, it was not straightforward to relate the qualitative interview data with the quantitative survey data for those project members who participated in both components of the study. Researchers can benefit from tools that are able to integrate the disparate methodological components involved in studying global teams.

## 8.9 Limitations and Future Work

This work reports on knowledge workers from a single corporation. Similar studies need to be conducted at other organizations in order to verify the applicability of these findings across different types of knowledge work firms. As far as the generalizability to other Indian knowledge work firms is concerned, informal consultations with several Indian knowledge workers from other firms suggest that our experience might be typical across most knowledge workplaces in India. Therefore, we believe that these results would apply more broadly beyond the firm we studied. Future studies are needed to investigate and compare across Indian work sites of different organizations.

# Chapter 9

# Contributions

Our research on reconciliation of privacy and awareness needs in loosely coupled collaboration began with an extensive investigation of IM as a representative IAIS employed in collaborative work. Subsequent studies verified the applicability of the results of the IM studies to other IAIS and contributed additional relevant findings. Moreover, reflections on our methodological experiences yielded several important insights for designing and conducting such studies. This chapter relates the results of our investigations described in Chapters 6, 7, and 8 with the hypotheses and research questions outlined in Chapter 3:

## 9.1 Answers to Research Questions

In tackling the research questions, we confirmed as well as refined and extended some of the findings from prior work described in Section 2.2. Moreover, we uncovered several new insights. Below, we summarize the findings as they relate to each of the research questions.

**Q1: What is the nature of these concerns?**

Our work uncovered that interpersonal privacy concerns in collaborative work lie along three dimenstions: who, what, and when & where (see Section 6.1.3). We also discovered that privacy concerns are impacted by user understanding of technology and by transparency of system operation. The average levels of privacy concerns expressed on a 1-7 scale in all of our questionnaires (see Sections 6.2.1 and 8.6) fell somewhere in the middle. This underscores that most collaborators do not seek absolute privacy but rather an appropriate reconciliation of privacy and awareness. Moreover, we found that privacy concerns depend on several important situational characteristics (viz., issues, relationships, temporality, technology, and space) and, in turn, on how these characteristics are interpreted according to various influences (viz., self, team, site, organization, and cultural environment) (see Section 8.3).

**Q2: In what ways do privacy management practices manifest themselves when collaborators interact with IAIS, and with each other, through these systems?**

The privacy management framework that emerged from our data (see Section 8.3) illustrates that privacy management occurs by applying one or more interpretive influences to one or more of the situational characteristics at hand. The choice and priority of the situational characteristics and interpretive influences leading to a particular privacy management decision vary based on the person and the context. Feedback regarding the "success" of past privacy management actions leads to the evolution and refinement of the interpretive influences.

**Q3: Which privacy needs do current IAIS leave unfulfilled?**

We noted several shortcomings of current IAIS:

- Inadequate visibility (to oneself) of one's impression that is projected to others via IAIS,
- Coarse granularity for managing privacy as a result of preferences that apply globally,
- Lack of notification regarding the actions and conflicting preferences of others that might impact one's privacy, and
- Lack of control over archives of past interactions.

**Q4: How can privacy management in IAIS be improved?**

To overcome the shortcomings described above, we designed and built a prototype that provides the following privacy-enhancing functionalities: notice, negotiation, control over conversation archives, expiration of contacts, encryption of channels and archives, visualization of collective activities, and group-level preference specification. User evaluation of the prototype demonstrates the utility of the designs for improving IAIS privacy management. The results from our study of a corporate awareness application (see Section 7.3) also show that group-level preference specification as well as increased transparency of system operation enhance privacy management.

## 9.2 Verification of Hypotheses

Based on the answers to our research questions, we revisit the hypotheses from Chapter 3.

**H1: In IAIS used for supporting loosely coupled collaboration, effective and seamless reconciliation of awareness needs and privacy desires could alleviate privacy concerns without unduly compromising the**

**benefits of awareness.**

The answers to Q3 highlighted several shortcomings of current IAIS that hamper effective reconciliation of privacy and awareness. As the answers to Q4 show, we were able to enhance privacy management by designing solutions to tackle these shortcomings. User agreement regarding the effectiveness of our design ideas for improving privacy management (see Sections 6.5 and 7.3) provides support for the verification of H1.

**H2: Impression management (Goffman, 1959) is an underlying cause of privacy concerns in IAIS.**

Based on the literature, we formulated a model that postulated the desire for impression management as an underlying cause of privacy desires (see Section 6.1.5). Using the answers to Q1 coupled with the literature, we operationalized the model using questionnaire items (see Section 6.2.1). We were able to verify H2 by establishing the validity of the model using linear structural modeling (see Section 6.2.1). While the model was verified based on responses to a questionnaire on a specific type of IAIS (viz., IM), its broader applicability to loosely coupled collaborative practices is demonstrated by the impression management practices described by the participants in our field study (see Section 8.5).

## 9.3 Additional Contributions

In addition, this work has also generated the following useful results:

- We uncovered a host of factors that influence privacy attitudes and practices in IAIS. Among these, the factors that have received little prior attention include:

user understanding of how technology works, transparency of system operation, and visibility (to oneself) of one's impression that is projected to others through the system.

- We highlighted situational characteristics (viz., issues, relationships, temporality, technology, and space) and interpretive influences (viz., self, team, site, organization, and cultural environment) that are important for privacy management.

- We identified differences in interpersonal privacy concerns among collaborators in the U.S. and India and described five factors that lead to the observed differences: physical characteristics of the workplace, nature of interpersonal relationships, conceptualization of privacy, intra-team competition, and management style and hierarchy.

- We provided useful insights for conducting usability evaluation of privacy designs and for studying globally distributed software teams.

# Appendices

## A IM Online Questionnaire

1. Are you currently employed?
    - Full-time (40 hours/week or more)
    - Part-time
    - Not currently employed
    - Other – Please specify:
2. Are you a student?
3. Why do you use Instant Messaging? (Check all that apply.)
    - It is required (or expected) at work.
    - It is required (or expected) at school.
    - To be more accessible to significant other
    - To determine the availability of specific people
    - To collaborate with local colleagues (peers, superiors and/or subordinates) at work

- To collaborate with geographically remote colleagues (peers, superiors and/or subordinates) at work
- To collaborate with classmates and/or professors at school
- To socialize with local friends
- To socialize with local family members
- To keep in touch with distant friends
- To keep in touch with distant family members
- To meet new people
- Other – Please specify:

4. Where do you use Instant Messaging from? (Check all that apply.)

    - Home
    - School
    - Work
    - Cyber cafe
    - Public library
    - Airport, Park, Coffee shop or other such locations where Internet access is available
    - Other – Please specify:

5. Which features of Instant Messaging do you use? (Check all that apply.)

    - Checking availability of contacts
    - Providing information regarding my own availability (e.g. with status/away messages)
    - Alerts regarding contacts signing on/off or changing status

- Individual chat with contacts
- Group (more than 2 people) chat
- Archive/saving of conversations
- Voice chat
- Webcam
- File transfer
- Application sharing
- New email alerts
- Other – Please specify:

6. Which Instant Messaging service(s) (i.e. network(s)) do you use? By service we mean a provider of an instant messaging network - such as MSN or ICQ - regardless of the specific client software you use to access the service. (Check all that apply.)

    - MSN
    - ICQ
    - Yahoo!
    - AOL
    - Private (e.g. Corporate or School internal network)
    - Other(s) – Please specify:

7. Do you have more than one account in any of the Instant Messaging services you use? (i.e. multiple accounts on the SAME Instant Messaging network.) Please indicate which Instant Messaging service(s) you have more than one account on? (Check all that apply.)

- MSN
- ICQ
- Yahoo!
- AOL
- Private (e.g. Corporate or School internal network)
- Other(s)

8. Why do you have more than one account? (Check all that apply.)
   - I use a separate account for different places (e.g. work, home)
   - I use a separate account for different sets of people (e.g. colleagues, family)
   - I use a separate account for different computers I use (e.g. desktop, laptop)
   - Other – Please specify:
9. Are there explicit policies at your school regarding the use of Instant Messaging?
   - Yes
   - No
   - Not sure
10. Do these policies alter the content and manner of your conversation?
    (1 = Never through 7 = Always)
    Please elaborate:
11. Are there explicit policies in your organization regarding the use of Instant Messaging?
    - Yes
    - No

- Not sure

12. Do these policies alter the content and manner of your conversation?
    (1 = Never through 7 = Always)
    Please elaborate:

13. What form(s) of communication do you use to discuss seemingly private or sensitive matters? (Check all that apply.)

    - Face-to-face
    - Land-line telephone
    - Cell phone
    - Email
    - Instant Messaging
    - Mail
    - I have never had to discuss private or sensitive matters.
    - Other – Please specify:

14. How concerned are you regarding privacy when using Instant Messaging? (1 = Not at all through 7 = Extremely)
    Please explain your reasons for the above level of concern:

15. Have you ever switched from Instant Messaging to another communication form(s) for seemingly private or sensitive discussions?
    If yes, please indicate why. (Check all that apply.)

    - It was difficult to communicate what I wanted to say via text conversation.
    - It was difficult to express feelings and emotions in Instant Messaging.
    - The communication involved multiple people.

- I did not want the conversation being saved or archived.
- I did not want the conversation being grabbed off the network by network admins, hackers, or other unknown people.
- Another form of communication was more efficient than Instant Messaging.
- I needed time to compose and revise my thoughts rather than instant communication.
- Other – Please specify:
- It's a bit more complicated. – Please elaborate below:

16. Do you maintain a profile with information about you in any of your Instant Messengers?

    - Yes, publicly accessible by anyone
    - Yes, but accessible only by my contacts
    - Not sure
    - No

    Please elaborate:

17. Do you use encryption for your Instant Messaging?

    - Yes
    - No
    - Not sure

18. Are you aware that (unencrypted) Instant Messaging conversations can be intercepted on the network by almost anyone (e.g network admins, hackers, or other strangers)?

    - Yes

- No
- Not sure

19. Does the fact that (unencrypted) Instant Messaging conversations can be intercepted on the network by almost anyone alter the content and manner of your conversation? (1 = Never through 7 = Always)
    Please elaborate:

20. Do you ever have multiple instant messaging conversations going on at the same time?

21. Have you ever sent a message to the wrong person (i.e. typed into the wrong window)? If yes, indicate what happened. (Check all that apply.)

    - I was embarrassed.
    - The other person was embarrassed.
    - I accidentally revealed private information to someone who should not have known it.
    - I accidentally revealed personal information to a person who had no connection to the matter.
    - Nothing happened as the content of the message was not personal or private.
    - Other – Please specify:

22. Have you ever received link to an inappropriate Website over Instant Messaging?

    - Yes, from a contact
    - Yes, from a stranger
    - No

23. Have you ever received a virus via Instant Messaging?

    - Yes, from a contact
    - Yes, from a stranger
    - No

24. How concerned are you regarding others looking at your computer screen while you are having an Instant Messaging conversation?
    (1 = Not at all through 7 = Extremely)
    Please elaborate:

25. What do you do if someone comes up to you while you are having an Instant Messaging conversation? (Check all that apply.)

    - Minimize all desktop windows
    - Minimize Instant Message conversation(s)
    - Keep conversation open but click on it to prevent blinking
    - Lock the screen
    - Turn off the screen
    - Turn on screensaver
    - Do nothing
    - Other – Please specify:
    - It depends – Please elaborate:

26. When you walk away from your computer for brief intervals, what do you typically do? (Check all that apply.)

    - I manually lock the computer,

- I have the computer set to lock automatically after a short period of inactivity
- I have the computer set to activate a password-protected screen-saver after a short period of inactivity,
- Nothing
- Other – Please specify:
- It's a bit more complicated. – Please elaborate:

27. When you are away from your computer for a brief interval, which of the following do you do regarding your Instant Messaging? (Check all that apply.)

    - I log out of Instant Messaging.
    - I manually set my status to "Away".
    - My Instant Messaging client automatically changes status to "Away" or "Idle" after a short period of inactivity.
    - My Instant Messaging client shows how long I have been "Away" or "Idle."
    - My Instant Messaging client automatically changes my display name to indicate I am "Away" or "Idle."
    - I use a default "Away Message" provided by the Instant Messaging client.
    - I use a custom or saved "Away message" I created myself.
    - Nothing
    - Other – Please specify:
    - It's a bit more complicated. – Please elaborate below:

28. Do you save your Instant Messaging conversations?

    - Never

- Yes, sometimes
- Yes, automatically

29. If you only save conversations on occasion, what prompts you to do so? (Check all that apply.)

    - Piece of information which might be needed later (e.g. the conversation contains an address)
    - Humorous content
    - Record-keeping (e.g. minutes of an online meeting)
    - Conversation needs to be shared with a third party
    - Other – Please specify:

30. Do you ever go back to any of your saved (or archived) Instant Messaging conversations?

    If yes, what prompts you to do so? (Check all that apply.)

    - Specific piece of information (e.g. the conversation contains an address)
    - Humorous content
    - Refreshing memory regarding previous conversation(s) before the next communication
    - Repeating whole or parts of a previous conversation to the contact
    - Sharing a conversation with a third party
    - Other – Please specify:

31. Are you aware of whether or not your contacts save the conversations they have with you?

    - Yes

- No
- Sometimes

32. Does the fact that your conversations could be saved by the other person alter the content and manner of your conversation?
    If yes, please explain your reasons. (Check all that apply.)

    - I am concerned that the conversation may be shared with a third person without my knowledge or permission.
    - I am concerned that the contents of the conversation may later be misconstrued.
    - I am concerned that the contents of the conversation may be taken out-of-context.
    - I am concerned that the contents of the conversation may be used against me.
    - I am concerned that the contents of the conversation may inadvertently be accessible to others (e.g. on a shared computer)
    - Other – Please specify:

33. Have you ever shared a conversation you had with someone with a third person?

    - Yes, with permission from the contact
    - Yes, without permission from the contact
    - No
    - It's a bit more complicated - Please elaborate below:

34. Has any of your contacts shared a conversation you had with them with a third person?

- Yes, with my permission
- Yes, without my permission
- Not sure
- No
- It's a bit more complicated - Please elaborate below:

35. If someone has shared one of your conversations with a third person without your permission, what was your reaction? (Check all that apply.)

    - I confronted the person.
    - I stopped talking to the person.
    - I was angry.
    - I felt that my trust was violated.
    - I felt that my privacy was violated.
    - I did not care as the content of the conversation was not private or sensitive.
    - I did not care as sharing the conversation was appropriate under the circumstance.
    - I did not particularly care, but I would not completely trust the person in the future.
    - Other – Please specify:

36. If someone shares one of your conversations with a third person without your permission, what would be your reaction? (Check all that apply.)

    - I would confront the person.
    - I would stop talking to the person.
    - I would be angry.

- I would feel that my trust was violated.
- I would feel that my privacy was violated.
- I would not care if the content of the conversation is not private or sensitive.
- I would not care as if sharing the conversation is appropriate under the circumstance.
- I would not particularly care, but I would not completely trust the person in the future.
- It depends on the person(s) involved.
- It depends on the situation.
- Not sure.
- Other – Please specify:

37. Indicate your level of comfort with the following groups of people being able to access and read all of your conversations (past, present or future).
(1 = Comfortable through 7 = Uncomfortable)

    - Friend
    - Family member
    - Colleague (peer)
    - Superior
    - Subordinate
    - Classmate
    - Significant other
    - Ex-significant other
    - Acquaintance

- Stranger

38. What best describes your availability in Instant Messaging?

    - My permission is needed for someone to add me to their contact list.
    - Anyone can add me to their contact list without my permission.
    - It's a bit more complicated. – Please elaborate:

39. Do you ever set your status to "Invisible" (i.e. no one can see that you are online)?

    If yes, please indicate why. (Check all that apply.)

    - I do not want to be bothered by anyone.
    - I do not want to be bothered by a specific person, but it was preferable to set my status to invisible than to block the person.
    - I want to watch availability of others without disclosing my own availability.
    - Being invisible allows me to message only the contacts I want without disclosing my availability/presence to others.
    - I have always-on Internet access, so being invisible prevents people messaging me when I am away from the computer for extended periods.
    - Other – Please specify:
    - It's a bit more complicated. – Please elaborate below:

40. Do you ever set your status to "Busy?"

    If yes, please indicate why. (Check all that apply.)

    - I do not want to be bothered by anyone.
    - I do not want to be bothered by a specific person, but it was preferable to set my status to busy than to block the person.

- I am working on something that requires high levels of concentration.
- I do not want my colleagues and/or superiors to think that I am not working hard.
- I do not want to be messaged by friends or family because I am at work.
- I only want to receive messages which need my immediate attention.
- Other – Please specify:
- It's a bit more complicated. – Please elaborate below:

41. How many contacts do you have in each of the Instant Messaging services you use?

    - MSN
    - ICQ
    - Yahoo!
    - AOL
    - Private (e.g. Corporate or School internal network)
    - Other

42. Do you have the same person on your contact list in more than one Instant Messaging service? (e.g. having the same person on your contact list in both MSN and ICQ networks.)

43. Do you have more than one contact entry for the SAME person on your contact list in the SAME Instant Messaging service? (e.g. having two entries for a contact who uses separate accounts from work and home.)

44. If you answered yes to any one of the above two questions, please indicate the TOTAL number of UNIQUE contacts in ALL of your Instant Messaging services combined.

45. Do you classify your contact list(s) into groups?

    - Yes, in each of the Instant Messaging services
    - Yes, but not in all of the Instant Messaging services
    - No

    If yes, why do you use grouping? (Check all that apply.)

    - I have so many people on my contact list that I need some way to organize.
    - Grouping makes it easier to find specific people on the contact list.
    - Other – Please specify:

    If no, why do you not use grouping? (Check all that apply.)

    - There are not enough people on my contact list to necessitate grouping.
    - I find it easier to sort contacts as online/offline, so there is no value in grouping.
    - I am not aware of grouping functionality.
    - Other – Please specify:

46. If you use grouping, please indicate the names of your groups in the Instant Messaging service(s) you use (e.g. Colleagues, Family, Friends, etc.)

47. How do you sort your contact list?

    - By group
    - By online/offline status
    - Alphabetically
    - Other – Please specify:

48. Have you ever blocked someone on your contact list?

49. Whom have you blocked? (Check all that apply.)

- Friend
- Family member
- Peer (colleague)
- Superior
- Subordinate
- Classmate
- Significant other
- Ex-significant other
- Acquaintance
- Stranger
- Other – Please specify:

50. For what reason(s) did you block the contact(s)? (Check all that apply.)

- The person was annoying me.
- The person said or did something to make me angry.
- The person moved.
- I moved.
- The person is no longer a part of my team/class/school/organization.
- I blocked the person by accident.
- A stranger had somehow ended up on my contact list.
- I was trying to avoid the person.
- I was trying to avoid the person. – Please elaborate.

- Other – Please specify:

51. Have you ever changed any default settings in the Instant Messaging client(s) you use?

    - I don't know.
    - No, I am happy with the defaults.
    - No, I would like to but I am unaware/unsure how.
    - Yes, during or right after installation.
    - Yes, during the period of initial use.
    - Yes, I change settings often. – Please explain:

52. Which setting(s) have you changed, and why?
    Please elaborate:

53. What has prompted (or prompts) you to change settings? (Check all that apply.)

    - I like to customize software I use to suit my practices.
    - I was browsing through the settings and found other settings that were more suited for me than the default choices.
    - I found some default setting(s) bothersome or annoying.
    - I wanted to emulate the settings of one of my contacts.
    - I wanted to change the settings to be available differently to specific individual(s).
    - A specific event prompted me to do so. – Please explain:
    - Other – Please specify:

54. Please indicate how important the addition of following features to Instant Messaging is to you?
(1 = Unimportant through 7 = Very important)

    - Ability to see how I appear to my contacts
    - Ability to see how I compare with my contacts based on my settings, conversations, and history
    - Ability to see what the other person is typing as each character is typed (rather than having to wait for them to press ENTER before you can view the entire line
    - Ability to specify settings on a per individual basis
    - Ability to specify settings on a per group basis
    - Ability to encrypt conversations
    - Ability to find out whether the other person saved the conversation
    - Ability to set expiry limits on archived conversations
    - No limit to the number of characters in each message
    - Ability to see who has added you to their contact list

55. If you could make any change to how Instant Messaging works presently, what would you add/remove/modify?

56. How long have you been using Instant Messaging? (By Instant Messaging, we mean any service or software - such as AOL Instant Messenger, ICQ, MSN Messenger - which allows you to find and/or communicate with others online.)

57. On average, approximately how much would you say are logged into one or more Instant Messaging services? (Please indicate the total time that you are LOGGED IN - in any mode, including invisible - even if you may not be actively

participating in any Instant Messaging conversations during the entire length of that time.)

58. What hardware do you use Instant Messaging on?(Check all that apply.)

    - Desktop
    - Laptop
    - Cell phone
    - PDA (e.g. PocketPC or Palm Pilot)
    - Other – Please specify:

59. Do you use any software which lets you log into multiple Instant Messaging services at the same time?

60. Why do you use this software? (Check all that apply.)

    - It is easier to manage accounts on different Instant Messaging services.
    - I no longer need to have multiple Instant Messaging clients running.
    - I can use a single interface for all Instant Messaging networks.
    - Other – Please specify:

61. How long have you been using the Internet?

    - Less than 6 months,
    - 6 months - 1 year
    - 1-2 years
    - 2-4 years
    - 4-8 years
    - More than 8 years

62. Where do you currently access the Internet from?

    - Home
    - School
    - Work
    - Cyber cafe
    - Public library
    - Airport, Park, Coffee shop or other such locations where Internet access is available
    - Other – Please specify:

63. For the place that you access the Internet from most often, please indicate the type of Internet connectivity you have.

    - Less than 6 months,
    - 6 months - 1 year
    - 1-2 years
    - 2-4 years
    - 4-8 years
    - More than 8 years

64. What kind of computer do you use to access the Internet at this place?

    - Desktop
    - Laptop
    - PDA (e.g. Palm Pilot, PocketPC etc.)
    - Cell phone

- Other - Please specify:

65. Is there anything else you would like to tell us?

66. How old are you?

67. What is your sex?

68. What is your marital status?

    - Married
    - Divorced
    - Separated
    - Single, never married
    - Single, but living with a partner
    - Single, but in a relationship
    - Single

69. Where are you located?

    - State & Country of residence
    - Country of citizenship

70. If you work, what is your profession?

    - Job title
    - Industry

71. If you are a student, what is the type of institution you attend?

    - High school
    - Community college

- College or University (undergraduate)
- College or University (graduate)
- Other – Please specify:

72. If you attend community college, college, or university, what is/are your field(s) of study? (e.g. Sociology)

# B Project X Online Questionnaire

1. On a scale of 1 (Strongly disagree) to (7=Strongly agree), please indicate your level of agreement with the following statements:

    - I find interruptions useful (e.g. to handle urgent issues, to catch up with colleagues, to take a break etc.)
    - Tools that help me better manage my privacy with respect to others would be useful to me.
    - I would like to know how others perceive me based on my interactions with them.
    - Knowing about my activities in detail can aid my manager in helping me be more effective and efficient.
    - My judgement of the urgency of an issue matches with how urgent others perceive that issue to be.
    - When working from home, I try to limit my interactions with others.
    - I use saved emails as a memory aid.
    - I use saved emails to hold others accountable for what they have previously said.

- I am careful about what I write in email because it could be saved by others.
- I worry that my emails can be forwarded to others without my knowledge/permission.
- Urgency is the most important factor in deciding how I handle an issue.
- I am willing to spend time in configuring software if the configuration results in better managing my privacy with respect to others.
- I use saved instant messages (IMs) as a memory aid.
- I use saved IMs to hold others accountable for what they have previously said.
- I am careful about what I write in IM because it could be saved by others.
- I worry that my IMs can be forwarded to others without my knowledge/permission.
- When handling an urgent issue, I may engage in actions which I would not otherwise (e.g., calling someone after hours).
- Interruptions disrupt my workflow and decrease my productivity.

If you answered "Not applicable" to any of the statements above, please explain below:

2. Please indicate how concerned you are regarding your privacy when dealing with the following groups of people on a scale of 1 (completely unconcerned) to 7 (extremely concerned). ("Privacy" is a broad concept that can encompass a variety of concerns including but not limited to confidentiality, availability to others, sharing of one's location and activities, disclosure of personal information, non-work life etc. In any situation, different individuals may characterize privacy differently. Please use YOUR characterization in the answers below.)

- Members of your team at your site (EXCLUDING your manager)
- Members of your team at REMOTE sites (EXCLUDING your manager)
- Your manager
- Other peers in Project X at your site
- Other peers in Project X at REMOTE sites
- Higher-level managers in Project X (i.e., managers of your manager and above)
- Non Project X employees at your site
- Non Project X employees at REMOTE sites
- Staff you supervise (if applicable)
- IT, system administrators and technical support

Please indicate below any comments/explanation for your answers above regarding the levels of privacy concern:

3. On a scale of 1(Strongly disagree) to 5( Strongly agree), please indicate your level of agreement with the following statements:

    - If I had my way, I wouldn't let the other team members have any influence over issues that are important.
    - Members of my team show a great deal of integrity.
    - In these competitive times one has to be alert or a team member is likely to take advantage of you.
    - We are usually considerate of one another's feelings in our team.
    - There is no "team spirit" in my team.
    - I really wish I had a good way to oversee the work of the other team members.

- I would be comfortable giving the other team members a task or problem which was critical, even if I could not monitor them.
- We have confidence in one another in our team.
- I can trust my team members to lend me a hand if I need it.
- I do not feel accepted as a team member by the others in my team.
- I discuss non-work related matters with my team members.
- I cannot rely on my team members to fulfill their commitments.
- The culture of my team tends to be cooperative.
- The culture of my team tends to be competitive.
- The work of my coworkers is of high quality.
- My team has a sense that we can succeed in spite of barriers.

Please indicate below any comments/explanation for your answers above:

4. Please list below the ways in which you personally measure the success of your project. For each measure, indicate your personal rating regarding how well your project meets the measure on a scale of 1-5 with 1 (does not meet at all) to 5 (meets perfectly). (For example, Quality of Code: 4 would indicate that you believe that "quality of code" is a measure of success for your project, and that you believe your project meets this measure at level 4 on a scale from 1 to 5.)

5. How much do you worry that your work email will be read by someone besides the person you sent it to?
   (1=A lot, 2=Some, 3=Not very much, 4=Not at all)

6. How much do you worry that your personal email will be read by someone besides the person you sent it to?
   (1=A lot, 2=Some, 3=Not very much, 4=Not at all)

7. How much do you worry that someone might know what Web sites you've visited when you are using the corporate network?
   (1=A lot, 2=Some, 3=Not very much, 4=Not at all)

8. How much do you worry that someone might know what Web sites you've visited when you are using your home network?
   (1=A lot, 2=Some, 3=Not very much, 4=Not at all)

9. How concerned are you about threats to your personal privacy when you are online?
   (1=Very, 2=Somewhat, 3=Not very, 4=Not at all)

10. Generally speaking, would you say that most people can be trusted, or that you can't be too careful in dealing with people?
    (1=Most people can be trusted, 2=Can't be too careful in dealing with people, 3=Depents, 4=Don't know)

11. How important is it to you when you deal with Internet stores that those companies or organizations adopt and follow strong privacy protection policies?
    ( 1=Very, 2=Somewhat, 3=Not very, 4=Not at all)

12. How confident are you that the things you do online are private and will not be used by others without your permission?
    (1=Very, 2=Somewhat, 3=Not very, 4=Not at all)

13. Most companies today want to know about the individual interests and lifestyles of their customers so that they can tailor their marketing to each customer's personal preferences. In general, do you see such PERSONALIZED MARKETING as a good thing for consumers?

14. On a scale of 1=Strongly disagree, 5=Strongly agree, please indicate your level of agreement with the following statements:

- In dealing with strangers one is better off being cautious until they have provided evidence that they are trustworthy.
- Most people can be counted on to do what they say they will do.
- I am willing to give information about myself in order to receive an online experience truly personalized for me.
- It is safe to believe that in spite of what people say, most people are primarily interested in their own welfare.

15. Have you ever personally inquired about or looked to see whether a business or service you were thinking of using had any policies on how it would use the consumer information it collected [or not]?

16. Have you ever refused to give information to a business or company because you thought it was not really needed or was too personal?

17. Have you ever decided not to use or purchase something from a company because you weren't sure how they would use your personal information?

18. Have you ever done any of the following?

    - Asked a company to remove your name and address from any lists they use for marketing purposes.
    - Asked a company not to sell or give your name and address to another company.
    - Asked a company to see what personal information, besides billing information, they had about you in their customer records.

19. Have you ever personally been the victim of what you felt was an invasion of your privacy when using the Internet?

20. Please indicate your level of agreement with the following statements:
(1=Always true, 2=Mostly true, 3=Sometimes true, 4=Equally true and false, 5=Sometimes false, 6=Mostly false, 7=Always false)

- I find it hard to imitate the behavior of other people.
- My behavior is usually an expression of my true inner feelings, attitudes, and beliefs.
- At parties and social gatherings, I do not attempt to do or say things that others will like.
- I can only argue for ideas which I already believe.
- I can make impromptu speeches even on topics about which I have almost no information.
- I guess I put on a show to impress or entertain people.
- When I am uncertain how to act in a social situation, I look to the behavior of others for cues.
- I would probably make a good actor.
- I rarely seek the advice of my friends to choose movies, books, or music.
- I sometimes appear to others to be experiencing deeper emotions than I actually am.
- I laugh more when I watch a comedy with others than when alone.
- In groups of people, I am rarely the center of attention.
- In different situations and with different people, I often act like very different persons.
- I am not particularly good at making other people like me.
- Even if I am not enjoying myself, I often pretend to be having a good time.

- I'm not always the person I appear to be.
- I would not change my opinions (or the way I do things) in order to please someone else or win their favor.
- I have considered being an entertainer.
- In order to get along and be liked, I tend to be what people expect me to be rather than anything else.
- I have never been good at games like charades or improvisational acting.
- I have trouble changing my behavior to suit different people and different situations.
- At a party, I let others keep the jokes and stories going.
- I feel a bit awkward in company and do not show up quite as well as I should.
- I can look anyone in the eye and tell a lie with a straight face (if for a right end).
- I may deceive people by being friendly when I really dislike them.

21. Age

22. Sex

23. Country (or countries) of citizenship

24. Number of years you have lived in the United States

25. Marital Status

26. Number of children

27. Number of people living in your household (INCLUDING yourself)

28. Highest level of education you have completed

29. Other level of education

30. Major field of study

31. Job function

    - Software developer
    - Tester
    - Systems engineer
    - Architect
    - Manager
    - SCM
    - Project management
    - Other – Please specify:

32. When did you first start working for the corporation?

33. When did you first start working on Project X?

34. When did you stop working on Project X?

35. In a typical week, approximately what percentage of your work time do (did) you spend working on Project X?

# Bibliography


Ackerman, M. S. (2000). The Intellectual Challenge of CSCW: The Gap between Social Requirements and Technical Feasibility. *Human-Computer Interaction*, 15:179–203.

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

Ackerman, M. S., Starr, B., Hindus, D., and 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.

Acquisti, A. and Grossklags, J. (2006). Privacy and Rationality. *Privacy and Technologies of Identity*, pages 15–29.

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

Adams, A. and 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*, pages 214–221.

Agre, P. E. and Rotenberg, M., editors (1997). *Technology and Privacy: The New Landscape*. MIT Press, Cambridge, MA, USA.

Albright, J. M. (2001). *Impression Formation and Attraction in Computer Mediated Communication*. Ph.D. thesis, University of Southern California.

Altman, I. (1975). *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*. Brooks/Cole, Monterey, California.

Altman, I. (1977). Privacy Regulation: Culturally Universal or Culturally Specific? *Journal of Social Issues*, 3(3):66–84.

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*, pages 66–78, London, UK. Springer-Verlag.

Avrahami, D., Fussell, S. R., and Hudson, S. E. (2008). IM waiting: Timing and responsiveness in semi-synchronous communication. In *CSCW '08: Proceedings of the ACM 2008 Conference on Computer Supported Cooperative Work*, pages 285–294, New York, NY, USA. ACM.

Aycan, Z., Kanungo, R. N., and Sinha, J. B. P. (1999). Organizational Culture and Human Resource Management Practices. *Journal of Cross-Cultural Psychology*, 30(4):501–526.

Bardram, J. E. (2004). Applications of Context-aware Computing in Hospital Work: Examples and Design Principles. In *SAC '04: Proceedings of the 2004 ACM Symposium on Applied Computing*, pages 1574–1579, New York, NY, USA. ACM.

Becker, J. A. H. and Stamp, G. H. (2001). Impression management in chat rooms: A grounded theory model. *Communication Research*, 56(3):243–260.

Begole, J. B., Tang, J. C., Smith, R. B., and 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*, pages 334–343, New York, NY, USA. ACM.

Bellman, S., Johnson, E., Kobrin, S., and Lohse, G. (2004). International Differences in Information Privacy Concerns: A Global Survey of Consumers. *The Information Society*, 20(5):313–324.

Bellotti, V. (1996). What You Don't Know Can Hurt You: Privacy in Collaborative Computing. In *HCI '96: Proceedings of HCI on People and Computers XI*, pages 241–261, London, UK. Springer-Verlag.

Bellotti, V. (1997). Design for Privacy in Multimedia Computing and Communications Environments. In Agre, P. E. and Rotenberg, M., editors, *Technology and Privacy: The New Landscape*, pages 63–98. MIT Press, Cambridge, MA, USA.

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

Berendt, B., Günther, O., and Spiekermann, S. (2005). Privacy in E-commerce: Stated Preferences vs. Actual Behavior. *Communications of the ACM*, 48(4):101–106.

Birnholtz, J. P., Gutwin, C., and Hawkey, K. (2007). Privacy in the Open: How Attention Mediates Awareness and Privacy in Open-plan Offices. In *GROUP '07: Proceedings of the 2007 International ACM Conference on Supporting Group Work*, pages 51–60, New York, NY, USA. ACM.

Black, J. P., Segmuller, W., Cohen, N., Leiba, B., Misra, A., Ebling, M. R., and Stern, E. (2004). Pervasive Computing in Health Care: Smart Spaces and Enterprise Information Systems. In *MobiSys 2004: Proceedings of the Second International Conference on Mobile Systems, Applications, and Services*, Boston, MA, USA.

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):28–46.

Boyle, M., Edwards, C., and 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*, pages 1–10, New York, NY, USA. ACM.

Boyle, M. and Greenberg, S. (2005). The language of privacy: Learning from video media space analysis and design. *ACM Transactions in Computer-Human Interaction*, 12(2):328–370.

Bozeman, D. P. and Kacmar, K. M. (1997). A Cybernetic Model of Impression Management Processes in Organizations. *Organizational Behavior and Human Decision Processes*, 69(1):9–30.

Bradner, E., Kellogg, W. A., and Erickson, T. (1998). Babble: suporting Conversation in the Workplace. *SIGGROUP Bulletin*, 19(3):8–10.

Burgoon, J. K., Parrott, R., Le Poire, B. A., Kelly, D. L., Walther, J. B., and Perry, D. (1989). Maintaining and restoring privacy through communication in different types of relationships. *Journal of Social and Personal Relationships*, 6:131–158.

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

Cadiz, J. J., Gupta, A., and Grudin, J. (2000). Using Web Annotations for Asynchronous Collaboration Around Documents. In *CSCW '00: Proceedings of the 2000 ACM Conference on Computer Supported Cooperative Work*, pages 309–318, New York, NY, USA. ACM.

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

Campbell, A. J. (1997). Relationship Marketing in Consumer Markets: A Comparison of Managerial and Consumer Attitudes about Information Privacy. *Journal of Direct Marketing*, 11(3):44–57.

Carroll, J. M., Neale, D. C., Isenhour, P. L., Rosson, M. B., and McCrickard, D. S. (2003). Notification and Awareness: Synchronizing Task-oriented Collaborative Activity. *International Journal of Human-Computer Studies*, 58(5):605–632.

Chen, H.-G., Chen, C. C., Lo, L., and Yang, S. C. (2008). Online privacy control via anonymity and pseudonym: Cross-cultural implications. *Behaviour & Information Technology*, 27(3):229–242. DOI 10.1080/01449290601156817.

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

Cho, H., Rivera-Sánchez, M., and Lim, S. S. (2009). A Multinational Study on Online Privacy: Global Concerns and Local Responses. *New Media & Society*, 11(3):395–416.

Consolvo, S., Smith, I. E., Matthews, T., LaMarca, A., Tabert, J., and 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*, pages 81–90, New York, NY, USA. ACM.

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

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 99.4.1.

Danis, C. M. (2000). Extending the Concept of Awareness to Include Static and Dynamic Person Information. *SIGGROUP Bulletin*, 21(3):59–62.

De Croon, E. M., Sluiter, J. K., Kuijer, P. P. F. M., and Frings-Dresen, M. H. W. (2005). The Effect of Office Concepts on Worker Health and Performance: A Systematic Review of the Literature. *Ergonomics*, 48(2):119–134.

Dey, A. K., Salber, D., Abowd, G. D., and Futakawa, M. (1999). The Conference Assistant: Combining Context-Awareness with Wearable Computing. In *ISWC '99: Proceedings of the 3rd IEEE International Symposium on Wearable Computers*, page 21, Washington, DC, USA. IEEE Computer Society.

Diffie, W. and Hellman, M. E. (March 1979). Privacy and Authentication: An Introduction to Cryptography. *Proceedings of the IEEE*, 67(3):397–427.

Dommeyer, C. J. and Gross, B. L. (2003). What Consumers Know and What They Do: An Investigation of Consumer Knowledge, Awareness, and Use of Privacy Protection Strategies. *Journal of Interactive Marketing*, 17(2):34–51. DOI 10.1002/dir.10053.

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

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

Dourish, P. and Bly, S. (1992). Portholes: Supporting Awareness in a Distributed Work Group. In *CHI '92: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 541–547, New York, NY, USA. ACM.

Dourish, P., Grinter, E., Delgado de la Flor, J., and Joseph, M. (2004). Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem. *Personal Ubiquitous Computing*, 8(6):391–401.

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

Ellison, N., Heino, R., and Gibbs, J. (2006). Managing Impressions Online: Self-Presentation Processes in the Online Dating Environment. *Journal of Computer-Mediated Communication*, 11(2):415–441.

Espinosa, J. A., Cummings, J. N., Wilson, J. M., and Pearce, B. M. (2003). Team Boundary Issues Across Multiple Global Firms. *Journal of Management Information Systems*, 19(4):157–190.

Festinger, L. (1950). Informal Social Communication. *Psychological Review*, 57(5):251–282.

Festinger, L. (1954). A Theory of Social Comparison Processes. *Human Relations*, 7(2):117–140.

Fisher, D. and Dourish, P. (2004). Social and Temporal Structures in Everyday Collaboration. In *CHI '04: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 551–558, New York, NY, USA. ACM.

Fogarty, J., Lai, J., and Christensen, J. (2004). Presence and Availability in a Context Aware Communication Client. *International Journal of Human-Computer Studies*, 61(3):299–317.

Fowler, F. J. (2008). *Survey Research Methods*. Sage Publications, 4 edition.

Fox, S. (2000). Trust and Privacy Online: Why Americans Want to Rewrite the Rules. *Pew Internet & American Life Project*.

Froehlich, J. and Dourish, P. (2004). Unifying Artifacts and Activities in a Visual Tool for Distributed Software Development Teams. In *ICSE '04: Proceedings of the 26th International Conference on Software Engineering*, pages 387–396, Washington, DC, USA. IEEE Computer Society.

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 *CHI '92: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 27–35, New York, NY, USA. ACM.

Giacalone, R. A. and Rosenfeld, P., editors (1990). *Impression Management in the Organization*. Lawrence Erlbaum, Mahwah, NJ.

Glaser, B. G. and Strauss, A. L. (1967). *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Aldine Transaction, 8 edition.

Goffman, E. (1959). *The Presentation of Self in Everyday Life*. Doubleday, Garden City, New York.

González, V. M. and Mark, G. (2004). "Constant, Constant, Multi-tasking Craziness": Managing Multiple Working Spheres. In *CHI '04: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 113–120, New York, NY, USA. ACM.

Greenberg, S. and Rounding, M. (2001). The Notification Collage: Posting Information to Public and Personal Displays. In *CHI '01: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 514–521, New York, NY, USA. ACM.

Greene, K. (2000). Disclosure of chronic illness varies by topic and target: The role of stigma and boundaries in willingness to disclose. In Petronio, S., editor, *Balancing the Secretes of Private Disclosures*, pages 123–135. Lawrence Erlbaum Associates, Mahwah, New Jersey.

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

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

Grudin, J. (1988). Why CSCW Applications Fail: Problems in the Design and Evaluation of Organizational Interfaces. In *CSCW '88: Proceedings of the 1988 ACM Conference on Computer-supported Cooperative Work*, pages 85–93, New York, NY, USA. ACM.

Haans, A., Kaiser, F. G., and de Kort, Y. A. W. (2007). Privacy Needs in Office Environments: Development of Two Behavior-Based Scales. *European Psychologist*, 12(2):93–102.

Hammersley, M. and Atkinson, P. (2007). *Ethnography: Principles in Practice*. Routledge, 3 edition.

Hancock, J. T. and Dunham, P. J. (2001). Impression formation in computer-mediated communication revisited: an analysis of the breadth and intensity of impressions. *Communication Research*, 28(3):325–347.

Harris & Associates, L. and Westin, A. F. (1998). Ecommerce & Privacy: What Net Users Want. *Privacy and American Business*.

Heath, C. and Luff, P. (1991). Disembodied Conduct: Communication Through Video in a Multi-Media Office Environment. In *CHI '91: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 99–103, New York, NY, USA. ACM.

Herbsleb, J. D., Atkins, D. L., Boyer, D. G., Handel, M., and 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*, pages 171–178, New York, NY, USA. ACM.

Hindus, D., Ackerman, M. S., Mainwaring, S., and Starr, B. (1996). Thunderwire: A Field Study of an Audio-only Media Space. In *CSCW '96: Proceedings of the 1996 ACM Conference on Computer Supported Cooperative Work*, pages 238–247, New York, NY, USA. ACM.

Hofstede, G. (2001). *Culture's Consequences, Comparing Values, Behaviors, Institutions, and Organizations Across Nations*. Sage Publications, Thousand Oaks, CA.

Hofstede, G. (2004). *Cultures and Organizations: Software of the Mind*. McGraw-Hill, U.S.A.

Hong, J. I., Ng, J. D., Lederer, S., and 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*, pages 91–100, New York, NY, USA. ACM Press.

Hsieh, G., Tang, K., Low, W., and Hong, J. (2007). Field Deployment of IMBuddy : A Study of Privacy Control and Feedback Mechanisms for Contextual IM. In Krumm, J., Abowed, G. D., Seneviratne, A., and Strang, T., editors, *UbiComp 2007: Ubiquitous Computing, 9th International Conference, Innsbruck, Austria*, pages 91–108. Springer Verlag.

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

Hudson, S. E. and 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*, pages 248–257, New York, NY, USA. ACM.

Hudson, James M. and Christensen, Jim and Kellogg, Wendy A. and Erickson, Thomas (2002). "I'd be overwhelmed, but it's just one more thing to do": Availability and Interruption in Research Management. In *CHI '02: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 97–104, New York, NY, USA. ACM.

Iachello, G. and 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*, pages 91–100, New York, NY, USA. ACM Press.

IBM (1999). IBM Multi-National Consumer Privacy Survey.

INRA (1997). Information Technology and Privacy. Report produced for the European Commission, Directorate General "Internal Market and Financial Services". Technical Report Eurobarometer 46.1, International Research Associates.

Introna, L. D. (1997). Privacy and the computer: Why we need privacy in the information society. *Metaphilosophy*, 28(3):259–275.

Introna, L. D. and Pouloudi, A. (1999). Privacy in the information age: Stakeholders, interests and values. *Journal of Business Ethics*, 22(1):27–38.

Ipsos Reid (2006). Global privacy of data: International survey.

Jarvenpaa, S. L., Knoll, K., and Leidner, D. E. (1998). Is Anybody Out There?: Antecedents of Trust in Global Virtual Teams. *Journal of Management Information Systems*, 14(4):29–64.

Johnson, D. G. (1985). Computers and Privacy. In *Computer Ethics*. Prentice-Hall, Englewood Cliffs, NJ.

Johnson, J. L. (1989). Privacy and the judgement of others. *The Journal of Value Inquiry*, 23(15):157–168.

Jöreskog, K. G. and Sörbom, D. (1993). *Structural Equation Modeling with the SIMPLIS Command Language*. Lawrence Erlbaum Associates, Hillsdale, NJ.

Jöreskog, K. G. and Sörbom, D. (2003). LISREL 8.54. SSI Central.

Kacmar, K. M., Wayne, S. J., and Wright, P. M. (1996). Subordinate Reactions to the Use of Impression Management Tactics and Feedback by the Supervisor. *Journal of Managerial Issues*, 8(1):35–53.

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

Khandwalla, P. N. (1988). Organizational Effectiveness. In Pandey, J., editor, *Psychology in India: The State-of-the-art*, volume 3, pages 97–216. Sage, New Delhi, India.

Kidd, C. D., Orr, R., Abowd, G. D., Atkeson, C. G., Essa, I. A., MacIntyre, B., Mynatt, E. D., Starner, T., and Newstetter, W. (1999). The Aware Home: A Living Laboratory for Ubiquitous Computing Research. In *CoBuild '99: Proceedings of the Second International Workshop on Cooperative Buildings, Integrating Information, Organization, and Architecture*, pages 191–198, London, UK. Springer-Verlag.

Kobsa, A. (2007a). Privacy-enhanced personalization. *Communications of the ACM*, 50(8):24–33. DOI 10.1145/1278201.1278202.

Kobsa, A. (2007b). Privacy-enhanced web personalization. In Brusilovsky, P., Kobsa, A., and Nejdl, W., editors, *The Adaptive Web: Methods and Strategies of Web Personalization*, pages 628–670. Springer Verlag, Berlin Heidelberg New York. DOI 10.1007/978-3-540-72079-9_21.

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

Kobsa, A. and Teltzrow, M. (2005). Contextualized Communication of Privacy Practices and Personalization Benefits: Impacts on Users' Data Sharing and Purchase Behavior. In Martin, D. and Serjantov, A., editors, *Privacy Enhancing Technologies: Fourth International Workshop, PET 2004*, number LNCS 3424, pages 329–343. Springer. DOI 10.1007/11423409_21.

Kraut, R., Egido, C., and 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*, pages 1–12, New York, NY, USA. ACM Press.

Kumaraguru, P., Cranor, L. F., and Newton, E. (2005). Privacy Perceptions in India and the United States: An Interview Study. In *The 33rd Research Conference on Communication, Information and Internet Policy (TPRC).*

Kupritz, V. W. (1998). Privacy in the Work Place: The Impact of Building Design. *Journal of Environmental Psychology*, 18(4):341–356.

Kvale, S. and Brinkmann, S. (2008). *InterViews: Learning the Craft of Qualitative Research Interviewing*. Sage Publications, 2 edition.

Landesberg, M. K., Levin, T. M., Curtin, C. G., and Lev, O. (1998). Privacy Online: A Report to Congress. Technical report, 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*, pages 273–291, London, UK. Springer-Verlag.

Lau, T., Etzioni, O., and 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.

Leary, M. R. and Kowalski, R. M. (1990). Impression Management: A Literature Review and Two-component Model. *Psychological Bulletin*, 107(1):34–47.

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

Lederer, S., Mankoff, J., and Dey, A. K. (2003a). Towards a Deconstruction of the Privacy Space. In *Ubicomp 2003 Workshop on Ubicomp Communities: Privacy as Boundary Negotiation*.

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

Lederer, S., Mankoff, J., Dey, A. K., and Beckmann, C. (2003c). 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., and 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*, pages 385–394, New York, NY, USA. ACM.

Lessig, L. (1999). *Code and Other Laws of Cyberspace*. Basic Books, Inc., New York, NY, USA.

Loo, A. (2008). The Myths and Truths of Wireless Security. *Communications of the ACM*, 51(2):66–71.

Mantei, M. M., Baecker, R. M., Sellen, A. J., Buxton, W. A. S., Milligan, T., and 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*, pages 203–208, New York, NY, USA. ACM Press.

Mason, R. O. (1986). Four Ethical Issues of the Information Age. *MIS Quarterly*, 10(1):5–12.

Mathur, P., Aycan, Z., and Kanungo, R. N. (1996). Indian Organizational Culture: A Comparison between Public and Private Sectors. *Psychology and Developing Societies*, 8(2):199–222.

Milberg, S. J., Burke, S. J., Smith, H. J., and Kallman, E. A. (1995). Values, Personal Information Privacy, and Regulatory Approaches. *Communications of the ACM*, 38(12):65–74.

Millen, D. R., Feinberg, J., and Kerr, B. (2006). Dogear: Social Bookmarking in the Enterprise. In *CHI '06: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 111–120, New York, NY, USA. ACM.

Miller, J. G. and Bersoff, D. M. (1999). Development in the Context of Everyday Family Relationships: Culture, Interpersonal Morality and Adaptation. In Killen, M. and Hart, D., editors, *Morality in Everyday Life*, chapter 8, pages 259–282. Cambridge University Press.

Milne, G. R. and Boza, M.-E. (1999). Trust and Concern in Consumers' Perceptions of Marketing Information Management Practices. *Journal of Interactive Marketing*, 13(1):5–24. DOI 10.1002/(SICI)1520-6653(199924)13:1¡5::AID-DIR2¿3.0.CO;2-9.

Moore, D., Kurtzberg, T., Thomson, L., and Morris, M. (1999). Long and Short Routes to Success in Electronically Mediated Negotiations: Group Affiliations and Good Vibrations. *Organization Behavior and Human Decision Processes*, 77(1):22–43.

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

Neale, D. C., Carroll, J. M., and Rosson, M. B. (2004). Evaluating Computer-Supported Cooperative Work: Models and Frameworks. In *CSCW '04: Proceedings of the 2004 ACM Conference on Computer Supported Cooperative Work*, pages 112–121, New York, NY, USA. ACM.

Negley, G. (1966). Philosophical Views on the Value of Privacy. *Law and Contemporary Problems*, 31(2):319–325.

Norman, D. A. (1988). *The Design of Everyday Things*. MIT Press, 3 edition.

Olson, G. M. and Olson, J. S. (2000). Distance Matters. *Human-Computer Interaction*, 15(2/3):139–178.

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

Olson, J. S. and 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*, pages 419–427, New York, NY, USA. ACM.

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*, pages 17–24, New York, NY, USA. ACM.

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

Pankoke-Babatz, U. and Syri, A. (1997). Collaborative Workspace for Time Deferred Electronic Cooperation. In *GROUP '03: Proceedings of the 2003 International ACM SIGGROUP Conference on Supporting Group Work*, pages 187–196, New York, NY, USA. ACM.

Parikh, I. J. and Garg, P. K. (1990). Indian Organizations: Value Dilemmas in Managerial Roles. In Jaeger, A. M. and Kanungo, R. N., editors, *Management in Developing Countries*. Routledge, London, UK.

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

Patil, S. and 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. and 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*, pages 109–112, New York, NY, USA. ACM. DOI 10.1145/1099203.1099220.

Patil, S. and Kobsa, A. (2009). Why is evaluating usability of privacy designs so hard? Lessons learned from a user study of PRISM. In *iConference 2009*.

Patil, S. and Kobsa, A. (2010). Enhancing privacy management support in instant messaging. *Interacting with Computers*, In press.

Patil, S., Kobsa, A., John, A., Brotman, L. S., and Seligmann, D. (2009). Interpersonal Privacy Management in Distributed Collaboration: Situational Characteristics and Interpretive Influences . In *INTERACT 2009: 12th IFIP TC13 Conference on Human-Computer Interaction*, pages 143–156, Berlin/Heidelberg. Springer. DOI 10.1007/978-3-642-03658-3_19.

Patil, S. and 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*, pages 101–110, New York, NY, USA. ACM. DOI 10.1145/1054972.1054987.

Pinelle, D. and Gutwin, C. (2003). Designing for Loose Coupling in Mobile Groups. In *GROUP '03: Proceedings of the 2003 International ACM SIGGROUP Conference On Supporting Group Work*, pages 75–84, New York, NY, USA. ACM.

Podsakoff, P., MacKenzie, S., Lee, J., and Podsakoff, N. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, 88:879–903.

Prinz, W., Mark, G., and Pankoke-Babatz, U. (1998). Designing Groupware for Congruency in Use. In *CSCW '98: Proceedings of the 1998 ACM Conference on Computer Supported Cooperative Work*, pages 373–382, New York, NY, USA. ACM.

Rachels, J. (1975). Why Privacy Is Important. *Philosophy and Public Affairs*, 4(4):323–333.

Raento, M. and Oulasvirta, A. (2008). Designing for privacy and self-presentation in social awareness. *Personal and Ubiquitous Computing*, 12(7):527–542.

Richards, J. and Christensen, J. (2004). People in Our Software. *Queue*, 1(10):80–86.

Rotter, J. B. (1967). A New Scale for the Measurement of Interpersonal Trust. *Journal of Personality*, 35(4):651–665.

Samarajiva, R. (1997). Interactivity as though Privacy Mattered. In Agre, P. E. and Rotenberg, M., editors, *Technology and Privacy: The New Landscape*, pages 277–309. MIT Press, Cambridge, MA, USA.

Schermelleh-Engel, K., Moosbrugger, H., and Müller, H. (2003). Evaluating the Fit of Structural Equation Models: Tests of Significance and Descriptive Goodness-of-Fit Measures. *Methods of Psychological Research Online*, 8(2):23–74.

Schneider, D. J. (1981). Tactical self-presentations: Toward a broader conception. In Tedeschi, J. T., editor, *Impression Management: Theory and Social Psychological Research*, pages 23–40. Academic Press, New York.

Schwartz, B. (1968). The Social Psychology of Privacy. *The American Journal of Sociology*, 73(6):741–752.

Sinha, J. B. P. (1982). Power in Indian Organization. *Indian Journal of Industrial Relations*, 17:339–352.

Sinha, J. B. P. (1990). *Work Culture in Indian Context*. Sage.

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

Snyder, M. (1974). Self-monitoring of Expressive Behavior. *Journal of Personality and Social Psychology*, 30(4):526–537.

Stokols, D., Clitheroe, C., and Zmuidzinas, M. (2002). Qualities of Work Environments That Promote Perceived Support for Creativity. *Creativity Research Journal*, 14(2):137–147.

Stone, E. F., Gueutal, H. G., Gardner, D. G., and McClure, S. (1983). A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes Across Several Types of Organizations. *Journal of Applied Psychology*, 68(3):459–468.

Sundstrom, E., Town, J. P., Brown, D. W., and Mcgee, C. (1982). Physical Enclosure, Type of Job, and Privacy in the Office. *Environment and Behavior*, 14(4):543–559.

U.S. Department of Health Education and Welfare (1973). Records, Computers and the Rights of Citizens. *Report of the Secretary's Advisory Committee on Automated Personal Data Systems*, Publication No. 1700–00116.

Voida, A., Grinter, R. E., Ducheneaut, N., Edwards, W. K., and Newman, M. W. (2005). Listening In: Practices Surrounding iTunes Music Sharing. In *CHI '05: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 191–200, New York, NY, USA. ACM.

Voida, A., Newstetter, W. C., and Mynatt, E. D. (2002). When Conventions Collide: The Tensions of Instant Messaging Attributed. In *CHI '02: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 187–194, New York, NY, USA. ACM.

Want, R., Hopper, A., Falcão, V., and Gibbons, J. (1992). The Active Badge Location System. *ACM Transactions on Information Systems*, 10(1):91–102.

Warren, S. D. and Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, 4(5):193–220.

West, R., Wright, G., and Graham, C. (2005). Blogs, Wikis, and Aggregators: A New Vocabulary for Promoting Reflection and Collaboration in a Preservice Technology Integration Course. In Crawford, C., Willis, D. A., Carlsen, R., Gibson, I., McFerrin, K., Price, J., and Weber, R., editors, *Proceedings of Society for Information Technology and Teacher Education International Conference 2005*, pages 1653–1658, Phoenix, AZ, USA. AACE.

Westin, A. F. (1967). *Privacy and Freedom.* Atheneum, New York.

Westin, A. F. (1991). Harris-Equifax Consumer Privacy Survey 1991.

Whitten, A. and Tygar, J. D. (1999). Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *8th USENIX Security Symposium.*

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

Yan, H. and Selker, T. (2000). Context-aware Office Assistant. In *IUI '00: Proceedings of the 5th International Conference on Intelligent User Interfaces*, pages 276–279, New York, NY, USA. ACM.

Zhang, Y. J., Chen, J. Q., and Wen, K.-W. (2002). Characteristics of Internet Users and Their Privacy Concerns: A Comparative Study Between China and the United States. *Journal of Internet Commerce*, 1(2):1–16.

Zuckerberg, M. (2006). An open letter from Mark Zuckerberg. http://blog.facebook.com/blog.php?post=2208562130.