

Privacy in Instant Messaging: An Impression Management Model

Alfred Kobsa^{1*}, Sameer Patil¹, Bertolt Meyer²

¹) Department of Informatics, University of California, Irvine, CA, 92697, USA

²) Psychologisches Institut der Universität Zürich, Switzerland

November 28, 2009

Abstract

Instant Messaging (IM) has evolved into an important tool for collaborative work that supports informal near-synchronous communication and fosters awareness of the online presence of one's communication partners. Like all awareness systems, IM runs into concerns regarding privacy. Drawing upon prior literature and exploratory interviews, we postulate a model that posits impression management as the underlying cause for privacy desires of IM users. We verify the model using Linear Structural Modeling on data from a large online survey of IM users across the U.S. The model establishes that the desire for privacy in IM arises due to the desire for impression management (both directly, as well as indirectly through the desire for visibility of one's impression to oneself). Based on this model, we suggest that IM systems could support privacy needs of users better by providing them with more knowledge and control over aspects that affect their IM-conveyed impression on others (i.e., by making impression management functionality available). Specifically, to help make and sustain appropriate impressions on IM contacts, IM systems should allow for increased visibility of one's actions to oneself, facilitate easy comparison of one's practices with those of others, and allow one to view oneself from the perspective of others as well as make finer-grained adjustments to IM settings than is possible today.

Keywords: Instant Messaging (IM), privacy, impression management, self presentation, visibility of impression, linear structural model

*Corresponding author. Email kobsa@uci.edu, phone +1 949 202-5704, fax +1 484 762-6644

1 Introduction

While Instant Messaging (IM) was originally popularized by adolescents who embraced it for maintaining social ties among friends (Grinter and Palen, 2002; Boneva *et al.*, 2004; Grinter *et al.*, 2006), its utility for collaborative work soon became apparent (Nardi *et al.*, 2000; Herbsleb *et al.*, 2002). IM serves the dual purpose of providing presence awareness and enabling informal near-synchronous communication. Both can improve the effectiveness of collaborative work. IM enables one to gauge the availability of colleagues and to channel one's communication accordingly. This facilitates faster turnaround for quick, short queries. It can also foster greater informal interaction among co-workers, no matter whether they are local or remote. Increased informal communication is known to have a positive effect on collaboration (Whittaker *et al.*, 1994; Kraut *et al.*, 1988). Unlike face-to-face meetings or telephone conversations, IM makes it easier to multi-task by maintaining multiple separate conversations simultaneously. Office workers who utilize IM also report communicating more frequently with co-workers electronically but feeling interrupted to a lesser extent than those who do not use IM (Garrett and Danzinger, 2008). Finally, IM can reduce the costs of long-distance communication, and of travel to meet with remote collaborators.

Since IM is so promising for improving collaborative work practices, Enterprise IM systems targeted towards organizational use are becoming part of corporate networks. Several companies have actively introduced IM into the daily work practices (Herbsleb *et al.*, 2002; Muller *et al.*, 2003). In many firms, IM is the medium of choice for quick informal business communication. While current business use of IM is mostly within one's organization, usage for communication and collaboration with external clients and business partners is increasing.

IM functionality has also been embedded in a number of other applications. Examples include web pages (e.g., Facebook), email clients (e.g., Apple Mail), and software development environments (e.g., Jazz, Cheng *et al.*, 2003). IM clients for mobile devices such as cellular phones and PDAs (Isaacs *et al.*, 2002) allow one to stay connected even when away from a conventional computer.

However, the utility of IM comes with privacy risks since both its awareness and communication sides create a tension with users' desire for privacy (Patil and Kobsa, 2004, 2005a). For instance, the increased visibility of one's online presence to others might lead to interruptions and distractions caused by inopportune incoming messages (Nielsen, 2003; González and Mark, 2004). Conversely, one may be perceived as unapproachable and uncooperative if one chooses to set one's IM status to "away" or "busy" for prolonged periods of time (Grinter and Palen, 2002; Grinter *et al.*, 2006). Moreover, one's IM conversations could be shared with third parties without one's permission or even knowledge (Festa, 2001; DD&eENL).

If privacy desires are not addressed effectively, resulting privacy concerns can become a barrier for the adoption and use of a software system. This is illustrated by a recent incident involving the popular social networking site Facebook, which introduced a new awareness feature that automatically presented to users an aggregation of every single activity of their friends. Tens of thousands of users were outraged. The revolt ranged from online petitions and protest groups to threats of a boycott (Calore, 2006). **Facebook eventually apologized and introduced privacy controls for these news feeds (Zuckerberg, 2006), but finally shut them down to settle a class-action lawsuit (Perez, 2009).**

In interviews with employees who use IM at work (Patil and Kobsa, 2004, 2005a), participants indeed reported feeling uneasy about the fact that their IM conversations could be saved, and possibly forwarded to others, without their knowledge. They were concerned that IM logs could be retrieved in the future, and misinterpreted due to the absence of the context in which their IM conversations were originally conducted. Respondents also complained about interruptions caused by their availability being broadcast through IM, and the resulting distraction. Moreover, they worried that their availability, as conveyed through IM, could be monitored by others and subsequently conclusions be drawn about their work productivity. As a matter of fact, one interviewee reported having been electronically stalked by a colleague who eventually reported her to management as being idle based on her IM status information.

From a corporate perspective, such privacy concerns may seem unwarranted. Companies have an interest in the transparency of employees' activities and availability, and in the preservation of conversations for knowledge management and accountability purposes. Our interviewees seemed to disagree to some extent, but did not openly fight company policies. Instead, they engaged in several selective information disclosure tactics aimed at preserving privacy, such as:

- selectively avoiding the use of IM (e.g., for potentially sensitive topics), and switching to a different communication medium instead;
- actively self-censoring what is said via IM;
- using IM merely in a perfunctory manner, to give the appearance of compliance;
- strategically changing one's IM status indicators to avoid interruptions;
- blocking IM contacts, in order to withhold information from them and avoid communication;
- creating multiple IM accounts to keep different activity spheres separate (e.g., work, school and home);
- disabling the saving of IM conversations on one's local machine, to avoid the risk of unauthorized and/or accidental access in the future; and
- negotiating an appropriate etiquette for sharing conversations with third parties.

These observed privacy concerns of IM users, and their resultant privacy-preserving strategies for selective information disclosure, underscore the need to enhance the support for privacy management in IM systems. As IM gains wider adoption and becomes richer in features, it needs to be ensured that its utility and promise are not undermined by underutilization or circumvention owing to privacy concerns (**Harrington and Beard, 1996**). To achieve this objective, we must first understand the nature of privacy desires of IM users, and specifically what factors influence these desires. Such an understanding could then help design enhancements to IM systems that avert or

alleviate privacy concerns. This paper presents the model of privacy desires that emerged from our studies. Our prior interviews had revealed tight links between privacy desires in Instant Messaging and people's desire to manage the impression they convey to others when using IM (Patil and Kobsa, 2004, 2005a). In the development of our model we therefore focused on the relationship between privacy and impression management.

2 Prior Research and Postulated Model

Our work bridges research on (1) privacy in awareness-supporting software systems, which is mostly conducted in the areas of Computer-Supported Collaborative Work, Computer-Mediated Communication and Ubiquitous Computing, and (2) impression management, which is mostly carried out in the areas of Social Psychology and Organizational Studies. We therefore review relevant literature from these two areas, which falls into four broad themes:

- 1a) user studies of awareness systems and the effects of those systems on privacy,**
- 1b) user studies of Instant Messaging systems including privacy issues,**
- 1c) conceptual research on privacy, specifically in computer-mediated interaction, and**
- 2) research on impression management.**

We discuss each of these themes in the subsections below, and thereupon formulate the hypotheses of our model.

2.1 User Studies of Awareness Systems

It has been known in the research community for quite some time that awareness systems engender what was generally identified as “privacy concerns”. Initial findings on users safeguarding privacy were primarily noted “on the side” in studies aimed at evaluating experiences with the awareness aspects of so-called “media spaces” Mantei *et al.* (1991). Dourish Dourish (1993) prepared the first

review of the privacy protections in a number of media spaces and characterizes privacy controls along a “social-technical continuum”. On the social end of this continuum, social pressures and norms are relied upon to prevent system abuse, while on its technical end, technology prevents attempted misuse. Social controls are likely to work well within small and relatively tight-knit communities only (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 though, such as turning off the system or altering one’s 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 they increase user trust that the system will protect their 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; Patil and Lai, 2005). Palen (1999) found that socio-technical mechanisms controlled privacy even in highly open network calendaring environments. Users managed privacy partly via technical access control, partly via the norm of reciprocity (e.g., “I will share my calendar with you, but only if you allow me to view your calendar as well”), partly via practices such as cryptic entries, omissions and defensive scheduling, and partly via social anonymity within the larger organizational context. Lee *et al.* (1997) suggest that users desire mechanisms that would 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 lightweight manner that “facilitates the tight coupling between the means to change privacy and the means to obtain feedback that privacy is attained.”

More recent studies on awareness systems have started targeting privacy as the primary object of investigation. A number of mechanisms have been implemented aimed at protecting users’ privacy in awareness systems (Hudson and Smith, 1996; Lederer *et al.*, 2003; Patil and Lai, 2005; Ignat *et al.*, 2008; Patil and Kobsa, 2010), and a number of factors have been unveiled that impact users’ privacy judgments. These factors 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.*, 2003; Patil and Kobsa, 2004, 2005a; Consolvo *et al.*, 2005; Olson *et al.*, 2005). Lederer *et al.* (2003) also showed that a-priori manual configuration of privacy preferences is better than automatic strategies, especially for information that users deem important.

2.2 User Studies of IM

Researchers have been studying IM from a variety of perspectives. Some have focused on specific user groups such as teens (Grinter and Palen, 2002; Boneva *et al.*, 2004; Grinter *et al.*, 2006), while others looked at specific domains such as the workplace (Isaacs *et al.*, 2002; Muller *et al.*, 2003; Garrett and Danzinger, 2008). There has also been work on the content (e.g., Volda *et al.*, 2002) and nature (e.g., Nardi *et al.*, 2000) of IM interactions. In contrast, Begole *et al.* (2002) looked at temporal patterns and other details of users' IM activity, in order to build predictive models.

Some of the mentioned work points to the existence of privacy concerns in IM usage. For instance, Herbsleb *et al.* (2002) found that privacy management mechanisms that place undue burdens on users constitute a barrier for the initial setup as well as the subsequent use of IM. Grinter and Palen (2002) and Grinter *et al.* (2006) found that teenagers made enterprising use of access permissions, profiles, status messages and screen names in order to manage privacy. Nardi *et al.* (2000) noticed that IM users frequently resorted to plausible deniability of physical presence as a means for privacy management.

2.3 Conceptual Research on Privacy

While research on privacy originated in the fields of law, psychology, sociology, communications, political science, architecture and urban design, it has since dramatically expanded into the computer and information sciences, organization and management research, economics, and the health sciences. A bibliometric analysis (Patil and Kobsa, 2009) revealed that the number of published non-fiction books and articles with “privacy” in their titles totals more than 20,000 since 1960. Of

these, nearly two thirds appeared in the past ten years alone. This dramatic rise in research productivity from the mid-1990s onwards (specifically in terms of research *articles* rather than books) coincides with the advent of the World Wide Web and e-commerce, which engendered widespread privacy concerns (see, e.g., Teltzrow and Kobsa, 2004).

From early on, privacy has been recognized to be a multi-faceted concept. Due to its individualized and subjective nature and its intricate interdependencies with the broader social, cultural and situational context, it eludes a universally agreed-upon definition (Altman, 1975, 1977; Young, 1978; Burgoon, 1982; Introna and Pouloudi, 1999; Solove, 2008). While the presence or lack of privacy is easy to identify when experienced in a concrete situation, “it seems that for every definition [of privacy] proposed by jurists and philosophers alike a counterexample can be found” (Introna, 1997). As Solove (2002) pointed out, the numerous definitions in the literature are however not completely independent from each other, but show “family resemblances” in terms of Wittgenstein (1953).

Patil and Kobsa (2009) review the three principal perspectives from which the different notions of privacy are commonly described and analyzed in the literature:

- The *normative perspective* sees privacy as a right or freedom, and studies the expediency of laws, principles and other norms in safeguarding privacy (e.g. Warren and Brandeis, 1890; Alderman and Kennedy, 1997; Solove *et al.*, 2005; Solove, 2006).
- The *social perspective* constructs privacy socially, based on the behavior and interaction of individuals as they conduct their day-to-day affairs (e.g., Westin, 1967; Burgoon, 1982; Petronio, 2002; Margulis, 2003).
- The *information-technical perspective* investigates how normative and social considerations can be operationalized in terms of the properties and functionality of information technology (e.g., Agre and Rotenberg, 1997; Cranor, 2002; Garfinkel and Rosenberg, 2006; Iachello and Hong, 2007).

Given the complexity of the notion of privacy, technology designers have found it difficult to translate the privacy-related findings of the various user studies into concrete system design guidance. Researchers have tried to address this problem by framing the theoretical insights into privacy in forms that are more amenable to system designers. For instance, Boyle and Greenberg (2005) describe a vocabulary 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 theory developed by social psychologist Irwin Altman (1975, 1977). It characterizes privacy as a dynamic and dialectic process of regulating the boundaries of disclosure, identity and temporality.

Developers of exploratory collaboration and awareness systems have further distilled general guidance on privacy into specific design principles for better privacy management in computer-mediated interaction and awareness. Bellotti and Sellen (1993) propose a design framework based on feedback and control regarding information capture, construction, accessibility and purposes. 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 define 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 in proposing that privacy-sensitive systems ought to appropriately notify users, seek consent, provide choice, allow anonymity or pseudonymity, 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, namely 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 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 that is used to implement the system. Finally, to incorporate user perceptions, Adams and Sasse (1999) propose a privacy model based on interacting concerns regarding information sensitivity, information receiver and information usage.

2.4 Impression Management

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 seminal work on self presentation (Goffman, 1959) 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.*, 2003; 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), and 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 awareness systems 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 above-mentioned records and awareness information¹.**
- The awareness information received by all targets is the same, even for those targets with whom one interacts rarely.
- 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 distinguish three separate types of impression in the context of awareness systems.

- 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.

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

- 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

2.5 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 intended 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 one's 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.

²The 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.

³Note 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.

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 awareness 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 1 shows the three hypotheses in a causal factor structure. We sought to test and quantify the hypothesized relations through linear structural modeling.

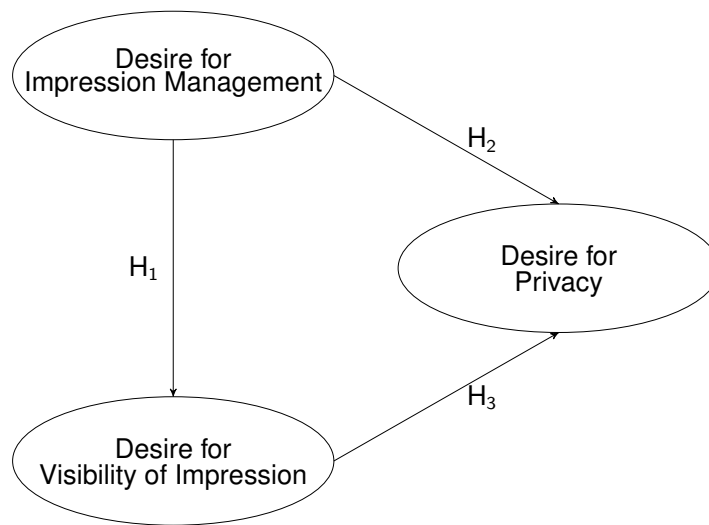


Figure 1: Hypothesized Causal Structure

3 Methodology

3.1 Scales

In order to verify the above hypotheses, 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 ques-

tionnaire 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), Patil and Kobsa (2004), and Patil and Kobsa (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 Likert 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.* (2003) and 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 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).

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	

Table 1: Assignment of Survey Questions to Constructs

3.2 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, standard deviations, and inter-item correlations are presented in table 2.**

	<i>M</i>	<i>SD</i>	(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 2: Means, standard deviations, and inter item correlations of measurement items ($N = 622$)

4 Factor Analysis and Linear Structural Modeling

4.1 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*.**

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.*, 2003; 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 2.**

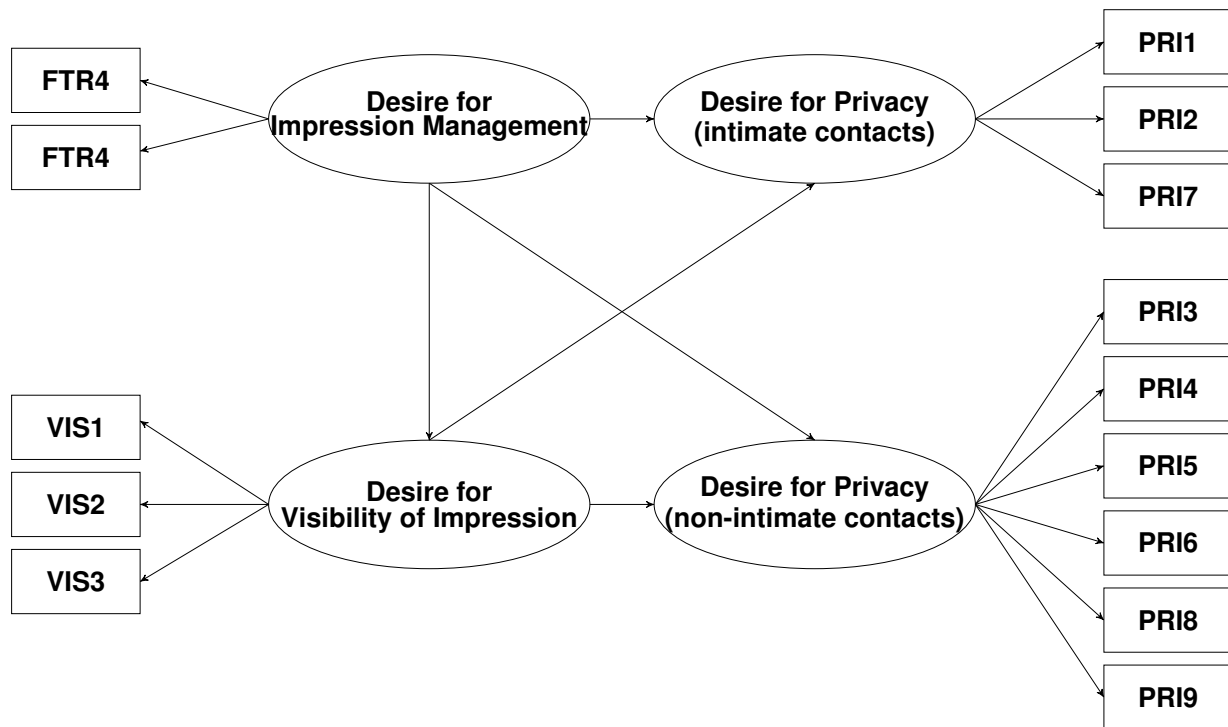


Figure 2: **Alternative hypothetical model including different desires for privacy with regard to the intimacy of contacts**

4.2 Linear Structural Modeling

We submitted both the original model (Figure 1) and the alternative model (Figure 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).

4.3 Results

The original structural model reached stable parameter estimates after fourteen iterations and is presented in Figure 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.**

Model	χ^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

Table 3: Goodness-of-Fit Statistics for The Original Model and the Alternative Model

Fit indices of both models are reported in Table 4.3. 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 4.3). 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 3. The model accounts for 9% of the variance in desire for privacy⁴ and for 26% of the variance in desire for visibility of impression.

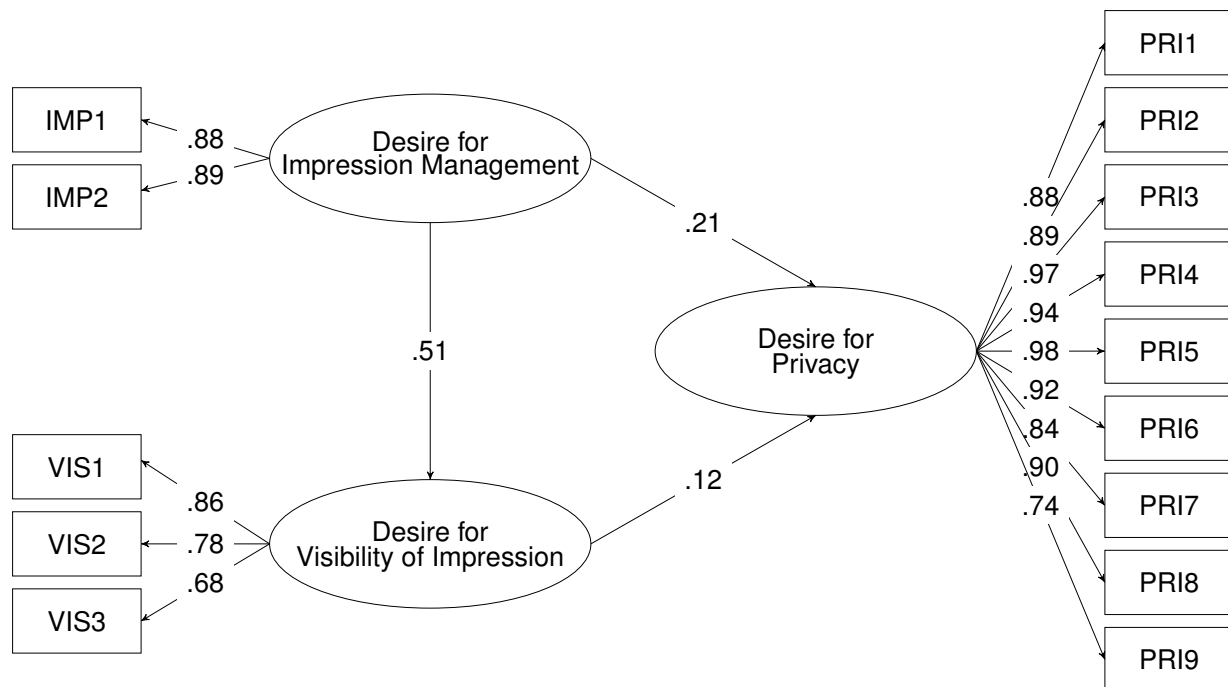


Figure 3: Path Diagram of the Linear Structural Equation Model with Path Coefficients

⁴This low amount of explained variance should come as no surprise since privacy is contingent on many situational and individual factors (see Section 2.3). 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) and Kobsa (2007b) for a review).

With acceptable model fit established, the assignment of measurement variables to constructs and the hypotheses can be evaluated. 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. Thus, the assumed factor structure (see Figure 3) can be found in the data.

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.

5 Discussion

5.1 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 ele-

mental 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.

5.2 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; 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.

6 Design Implications

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. 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.

6.1 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 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.

6.2 Better visibility of collective practices

Impression visibility also involves the desire of users to compare themselves against prevailing collective practices (see Table 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.

6.3 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.

6.4 Seeing the actually conveyed impression

The Faces system (Lederer *et al.*, 2003) 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.⁵ 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.

⁵Raento 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.

6.5 Towards a Privacy-Enhanced IM Client

In order to enhance current IM privacy management, we developed the PRISM (PRIVacy Sensitive Messaging) plugin for an open-source IM system, which incorporates some of the above design implications (Patil and Kobsa, 2010). 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 future work, we aim to explore the generalizability of our findings to awareness systems beyond IM.

7 Summary and Conclusion

Our study was motivated by the prevalence of privacy concerns that we encountered in interviews with IM users. Based on a qualitative analysis of these interviews we developed three theoretical constructs with associated measurement variables, namely desire to manage the impression one conveys to others, desire for visibility to oneself of the impression conveyed to others, and desire for privacy. Based on the research literature we postulated a causal relationship between desire for impression management and desire for privacy, both directly and also indirectly via the desire for visibility of one's impression. We validated our hypotheses on the basis of a geographically distributed survey of U.S. Internet users through linear structural modeling.

The results of our study imply that impression management should be taken into account much more seriously in the design of IM system than is currently the case, since impression management desire **clearly is a separate construct** that underlies the prevalent privacy desires in IM usage. Based on our model we propose four types of capabilities that IM systems should support, coarsely

ranked by increased value for users but also complexity of implementation:

- Better visibility of one's actions to oneself will allow IM users to obtain a better understanding of their own activities than is currently the case based on mere recollection.
- Better visibility of collective practices will allow IM users to compare their own activities with those of others.
- Fine-grained controls for impression management will allow them to convey different impressions to different contacts and groups of contacts.
- Seeing the actually conveyed impression, finally, would allow users to view themselves from the perspective of others.

These different kinds of information would help users gauge the impression they are likely to convey, while the fine-grained controls would allow them to exercise control over their impression on a per-group or even per-receipient basis.

Another more general result of the presented research 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. 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.⁶

8 Acknowledgments

Thanks are due to Heather Pulliam for her assistance in building the questionnaire, to all respondents, and to Marcel Paulssen who helped assess the quality of the linear structural model. We also thank Gillian Hayes, Mihir Mahajan, Gloria Mark, David Nguyen **and Xinru Page as well as the**

⁶One of the rare examples of such a privacy definition is from Johnson (1989), Introna (1997) and Introna and Pouloudi (1999), who characterize privacy as immunity from the judgment of others.

anonymous reviewers for their comments and suggestions. This research has been supported by NSF Grants No. 0205724 **and 0808783**, and by a Humboldt Research Award to the first author.

References

- Ackerman, M.S. and Cranor, L., 1999. Privacy Critics: UI Components to Safeguard Users' Privacy, in: *CHI '99 Extended Abstracts on Human Factors in Computing Systems*, New York, NY: ACM Press, 258–259.
- 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 Transactions in Computer-Human Interaction*, 4 (1), 39–66.
- Adams, A., 1999. Users' Perception of Privacy in Multimedia Communication, in: *CHI '99: CHI '99 Extended Abstracts on Human Factors in Computing Systems*, New York, NY: ACM Press, 53–54.
- 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*, 214–221.
- Agre, P.E. and Rotenberg, M., eds., 1997. *Technology and Privacy: The New Landscape*, Cambridge, MA: MIT Press.
- Albright, J.M., 2001. *Impression Formation and Attraction in Computer Mediated Communication*, Ph.D. thesis, University of Southern California.
- Alderman, E. and Kennedy, C., 1997. *The Right to Privacy*, New York, NY: Vintage.
- Altman, I., 1975. *The Environment and Social Behavior*, Belmont, CA: Wadsworth.
- Altman, I., 1977. Privacy Regulation: Culturally Universal or Culturally Specific?, *Journal of Social Issues*, 3 (3), 66–84.
- 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*, New York, NY, USA: ACM, 285–294.
- 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*, New York, NY: ACM Press, 334–343.
- 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*, London, UK: Springer-Verlag, 241–261.
- 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*, Norwell, MA: Kluwer Academic Publishers, 77–92.
- Boneva, B., Quinn, A., Kraut, R., Kiesler, S., and Shklovski, I., 2004. Teenage Communication in the Instant Messaging Era, *in: R. Kraut, M. Brynin, and S. Kiesler, eds., Information Technology at Home*, Oxford University Press.
- 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.
- Burgoon, J.K., 1982. Privacy and communication, *in: M. Burgoon, ed., Communication Yearbook 6*, Beverly Hills, CA: Sage Publications, 206–249.
- 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.
- Calore, M., 2006. Privacy Fears Shock Facebook, *Wired News*, <http://www.wired.com/science/discoveries/news/2006/09/71739>.
- 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*, New York, NY: ACM Press, 45–49.

- 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*, New York, NY: ACM Press, 81–90.
- Cranor, L.F., 2002. *Web Privacy with P3P*, Sebastopol, CA: O'Reilly & Associates, Inc.
- DD&eNL, 2003. Instant Messages Emerging as Newest Source of E-evidence, *Digital Discovery & e-Evidence Newsletter*, 3 (9), 1–3, <http://sochaconsulting.com/Publications/DDEE%%2009.03.pdf>.
- Dourish, P., 1993. Culture And Control In A Media Space, in: *ECSCW'93: Proceedings of the Third European Conference on Computer-Supported Cooperative Work*, Norwell, MA: Kluwer Academic Publishers, 125–137.
- 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.
- Festa, P., 2001. ICQ logs spark corporate nightmare. <http://www.news.com/2100-1023-254173.html&tag=st.cn.1.lthd>.
- 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.
- Garfinkel, S. and Rosenberg, B., eds., 2006. *RFID : Applications, Security, and Privacy*, Upper Saddle River, NJ: Addison-Wesley.
- Garrett, R.K. and Danzinger, J.N., 2008. IM = Interruption Management? Instant Messaging and Disruption in the Workplace, *Journal of Computer-Mediated Communication*, 13 (1), 23–42.
- Giacalone, R.A. and Rosenfeld, P., eds., 1990. *Impression Management in the Organization*, Mahwah, NJ: Lawrence Erlbaum.
- Goffman, E., 1959. *The Presentation of Self in Everyday Life*, Garden City, New York: Doubleday.
- González, V.M. and Mark, G., 2004. “Constant, Constant, Multi-tasking Crazyiness”: Managing Multiple Working Spheres, in: *CHI '04: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, New York, NY: ACM Press, 113–120.

- Greene, K., 2000. Disclosure of chronic illness varies by topic and target: The role of stigma and boundaries in willingness to disclose, *in: S. Petronio, ed., Balancing the Secretes of Private Disclosures*, Mahwah, New Jersey: Lawrence Erlbaum Associates, 123–135.
- 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*, New York, NY: ACM Press, 21–30.
- Grinter, R.E., Palen, L., and Eldridge, M., 2006. Chatting with Teenagers: Considering the Place of Chat Technologies in Teen Life, *ACM Transactions in Computer-Human Interaction-Hum. Interact.*, 13 (4), 423–447.
- 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.
- Harrington, K.V. and Beard, J.W., 1996. The appropriate use of computer-based information technologies: an impression management framework, *in: J.W. Beard, ed., Impression Management and Information Technology*, Westport, CT: Quantum Books, 133–157.
- 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*, New York, NY: ACM Press, 171–178.
- 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*, New York, NY: ACM Press, 91–100.
- 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: J. Krumm, G.D. Abowed, A. Seneviratne, and T. Strang, eds., UbiComp 2007: Ubiquitous Computing, 9th International Conference, Innsbruck, Austria*, Springer Verlag, 91–108.
- 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*, New York, NY: ACM Press, 248–257.
- 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*, New York, NY: ACM Press, 91–100.
- Iachello, G. and Hong, J., 2007. End-User Privacy in Human-Computer Interaction, *Foundations and Trends in Human-Computer Interaction*, 1 (1), 1–137.
- IBM, 1999. IBM Multi-National Consumer Privacy Survey, http://www.ibm.com/services/files/privacy_survey_oct991.pdf.
- Ignat, C.L., Papadopoulou, S., Oster, G., and Norrie, M.C., 2008. Providing awareness in multi-synchronous collaboration without compromising privacy, in: *CSCW'08: Proceedings of the ACM 2008 Conference on Computer Supported Collaborative Work*, New York, NY: ACM Press, 659–668.
- INRA, 1997. Information Technology and Privacy. Report produced for the European Commission, Directorate General “Internal Market and Financial Services”, Tech. Rep. 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.
- Isaacs, E., Walendowski, A., and Ranganathan, D., 2002. Mobile Instant Messaging through Hub-bub, *Communications of the ACM*, 45 (9), 68–72.
- 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*, Hillsdale, NJ: Lawrence Erlbaum Associates.
- 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.
- 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: P. Brusilovsky, A. Kobsa, and W. Nejdl, eds., *The Adaptive Web: Methods and Strategies of Web Personalization*, Berlin Heidelberg New York: Springer Verlag, 628–670, DOI 10.1007/978-3-540-72079-9_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*, New York, NY: ACM Press, 1–12.
- Langheinrich, M., 2001. Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems, in: *UbiComp '01: Proceedings of the 3rd International Conference on Ubiquitous Computing*, London, UK: Springer-Verlag, 273–291.
- Leary, M.R., 1996. *Self-Presentation: Impression Management and Interpersonal Behavior*, Norwood, MA: Westwood Press.
- 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., 2003. Who Wants to Know What When? Privacy Preference Determinants in Ubiquitous Computing, in: *CHI '03 Extended Abstracts on Human Factors in Computing Systems*, New York, NY: ACM Press, 724–725.
- 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*, New York, NY: ACM Press, 385–394.
- 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*, New York, NY: ACM Press, 203–208.
- Margulis, S.T., ed., 2003. *Journal of Social Issues, Special Issue on Contemporary Perspectives on Privacy: Social, Psychological and Political*, Boston, MA: Blackwell Publishing.
- Muller, M.J., Raven, M.E., Kogan, S., Millen, D.R., and Carey, K., 2003. Introducing Chat into Business Organizations: Toward an Instant Messaging Maturity Model, in: *GROUP '03: Proceedings of the 2003 International ACM SIGGROUP Conference on Supporting Group Work*, New York, NY: ACM Press, 50–57.

- 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*, New York, NY: ACM Press, 79–88.
- Nielsen, J., 2003. IM, Not IP (Information Pollution), *ACM Queue*, 1 (8), 76–77.
- Olson, J.S., Grudin, J., and Horvitz, E., 2005. A Study of Preferences for Sharing and Privacy, in: *CHI '05 Extended Abstracts on Human Factors in Computing Systems*, New York, NY: ACM Press, 1985–1988.
- 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*, New York, NY: ACM Press, 17–24.
- 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*, New York, NY: ACM Press, 129–136.
- Patil, S. and Kobsa, A., 2004. Instant Messaging and Privacy, in: *Proceedings of HCI 2004*, 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: *Proceedings of 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: *Proceedings of the 2005 international ACM SIGGROUP Conference on Supporting Group Work*, ACM Press, 109–112, DOI 10.1145/1099203.1099220.
- Patil, S. and Kobsa, A., 2009. Privacy Considerations in Awareness Systems: Designing with Privacy in Mind, in: P. Markopoulos, B. de Ruyter, and W. Mackay, eds., *Awareness Systems: Advances in Theory, Methodology and Design*, Springer Verlag, 187–206, DOI 10.1007/978-1-84882-477-5_8.
- Patil, S. and Kobsa, A., 2010. Enhancing privacy management support in Instant Messaging, *Interacting with Computers (final submission)*, <http://dx.doi.org/10.1016/j.intcom.2009.10.002>.
- 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*, New York, NY: ACM Press, 101–110, DOI 10.1145/1054972.1054987.

- Perez, J.C., 2009. Facebook will shut down beacon to settle lawsuit, <http://www.networkworld.com/news/2009/091909-facebook-will-shut-down-beacon.html>.
- Petronio, S., 2002. *Boundaries of Privacy: Dialectics of Disclosure*, Albany, NY: State University of New York Press.
- 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.
- Raento, M. and Oulasvirta, A., 2008. Designing for privacy and self-presentation in social awareness, *Personal and Ubiquitous Computing*, 12 (7), 527–542.
- Reid, I., 2006. Global privacy of data: International survey, http://www.surveillanceproject.org/files/Ipsos_Report_Nov_2006.pdf.
- 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: J.T. Tedeschi, ed., *Impression Management: Theory and Social Psychological Research*, New York: Academic Press, 23–40.
- Solove, D.J., 2002. Conceptualizing privacy, *California Law Review*, 90, 1087–1115, <http://ssrn.com/abstract=313103>.
- Solove, D.J., 2006. A taxonomy of privacy, *University of Pennsylvania Law Review*, 154 (3), 477–564, <http://ssrn.com/abstract=667622>.
- Solove, D.J., 2008. *Understanding Privacy*, Cambridge, MA: Harvard University Press.
- Solove, D.J., Rotenberg, M., and Schwartz, P.M., 2005. *Information Privacy Law*, New York, NY: Aspen Publishers, 2nd ed.
- Teltzrow, M. and Kobsa, A., 2004. Impacts of user privacy preferences on personalized systems: a comparative study, in: C.M. Karat, J. Blom, and J. Karat, eds., *Designing Personalized User Experiences for eCommerce*, Dordrecht, Netherlands: Kluwer Academic Publishers, 315–332, dOI 10.1007/1-4020-2148-8_17.

- 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*, New York, NY: ACM Press, 187–194.
- Warren, S. and Brandeis, L.D., 1890. The right to privacy, *Harvard Law Review*, 4 (5), 193–220.
- Westin, A.F., 1967. *Privacy and Freedom*, New York, NY: Atheneum.
- Whittaker, S., Frohlich, D., and Daly-Jones, O., 1994. Informal workplace communication: What is it like and how might we support it?, *in: CHI '94: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, New York, NY: ACM Press, 131–137.
- Wittgenstein, L., 1953. *Philosophical Investigations*, Blackwell Publishing.
- Young, J.B., 1978. Introduction: A look at privacy, *in: J.B. Young, ed., Privacy*, Chichester, New York: John Wiley & Sons.
- 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*, 1-16 (2), 1.
- Zuckerberg, M., 2006. An open letter from Mark Zuckerberg, <http://blog.facebook.com/blog.php?post=2208562130>.