Proceedings of Group'05, 5th ACM Conference on Supporting Group Work, Sanibel Island, FL, 2005, 101-105.

Uncovering Privacy Attitudes and Practices in Instant Messaging

Sameer Patil, Alfred Kobsa
Department of Informatics
Donald Bren School of Information and Computer Sciences
University of California, Irvine CA 92697 USA
+1-949-485-5210, +1-949-485-5020
{patil, kobsa}@uci.edu

ABSTRACT

We present an analysis of privacy attitudes and practices in Instant Messaging based on responses to an online questionnaire. On a 7-point Likert scale, the reported concern about IM privacy spanned the whole range, with the average being slightly below "medium". Respondents' justifications for privacy concerns revealed that the main contributing factors were: sensitivity of content, personal disposition towards privacy, understanding of technology, and potential persistence of conversations. Expectations for various categories of contacts differed significantly. Our findings indicate that it may be useful to leverage grouping functionality for privacy management. We also propose making the underlying technology more transparent.

Categories and Subject Descriptors

H.5.3 [**Information Interfaces and Presentation (e.g., HCI)**]: Group and Organization Interfaces – *Collaborative computing, Computer-supported cooperative work.*

General Terms

Design, Human Factors.

Keywords

Privacy, Instant Messaging, IM, Chat, Computer-Mediated Communication, CMC.

1. INTRODUCTION

In recent years, Instant Messaging (IM) has emerged as a useful tool for communication and collaboration, at home as well as in the workplace [4, 6]. Awareness indicators in IM (i.e., indicators of a person's presence and availability) facilitate spontaneous communication in a lightweight manner. Some research studies of IM have found evidence that privacy issues are an important consideration. For instance, Herbsleb et. al. [3] described how their attempts to introduce IM in the workplace ran into thorny privacy considerations. Similarly, Grinter and Palen [2] illustrated the importance of privacy management in use of IM by teens.

Yet, to our knowledge, no empirical research has focused on concrete characterization of privacy concerns in IM. Such analysis can aid in designing effective remedies to alleviate privacy concerns of IM users, and will likely further enhance its popularity and utility as a collaboration and communication tool. As an essential first step towards devising solutions to mitigate privacy concerns, we attempted to uncover the causes and nature of such concerns, and to look at current user practices that aim at addressing these. With the advent of telecommuting and flexible work hours, the traditional boundaries between home and work are blurring; hence we decided to study IM use in general rather than limiting it to a particular context.

2. METHODOLOGY

We developed a detailed online questionnaire aimed at understanding privacy attitudes and practices of adult (18 years or older) IM users. 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. The questionnaire was developed based on prior semi-structured interviews of experienced IM users who were drawn from diverse contexts [7].

An announcement of the questionnaire was distributed via various mailing lists, personal contacts, and via postings to a large online community site (craigslist.org) which has local sites for most major cities and metropolitan areas 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 3 weeks.

A detailed analysis of the responses is in progress. In this paper, we focus on responses to three specific privacy-related questions. We asked 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 Likert scale along with an open-ended explanation for the rating. And 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 Likert scale for the categories we provided: friends, family, colleagues, superiors, subordinates, classmates, significant others, ex-significant others, acquaintances, and strangers.

GROUP'05, November 6th, 2005, Sanibel Island, Florida, USA.

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 of ratings into a list of categories that we had developed based on the responses. The two authors 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 agreement was reached.

3. FINDINGS

User-reported concern about IM privacy (see Figure 1) 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%)[1]. The relative frequencies of each of these four factors showed statistically significant correlations ($p < 0.05$) with rated privacy concern.

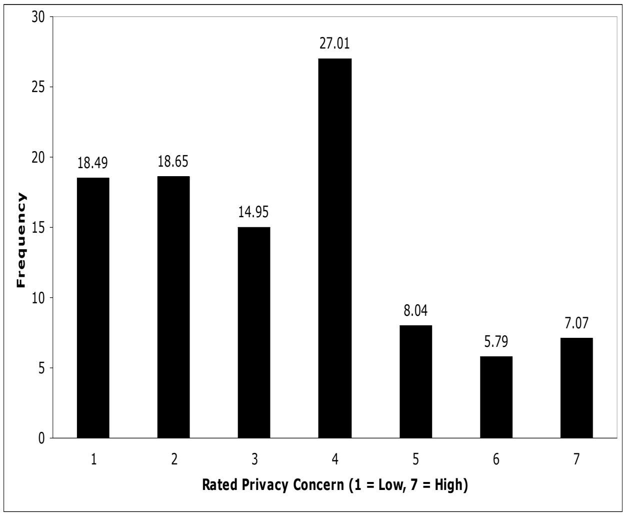

Figure 1. User-rated privacy concern on a 7-point Likert scale.

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 ($p \sim 0$ for not-sensitive & $p \sim 0.03$ for sensitive content, see Figure 2). Personal disposition towards privacy reflects a respondent's inherent attitudes. This encompassed comments in which respondents expressed "indifference" ($p \sim 0.001$) as well as those in which respondents claimed to "value privacy" ($p \sim 0.1$). The frequencies of these justifications seemed to even be exponential rather than linear (see Figure 3). 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).

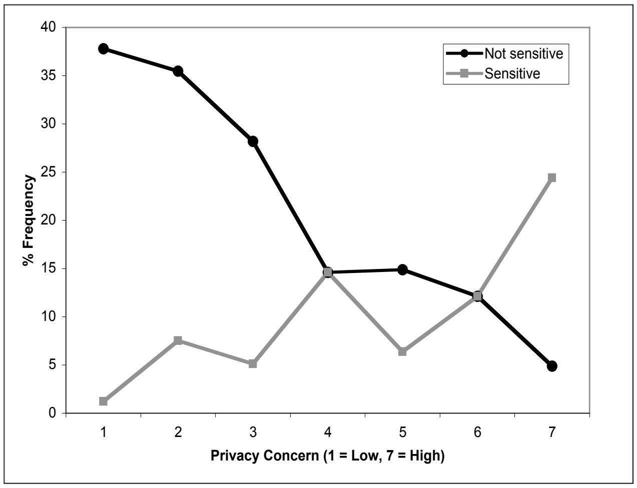

Figure 2. Impact of sensitivity of conversation.

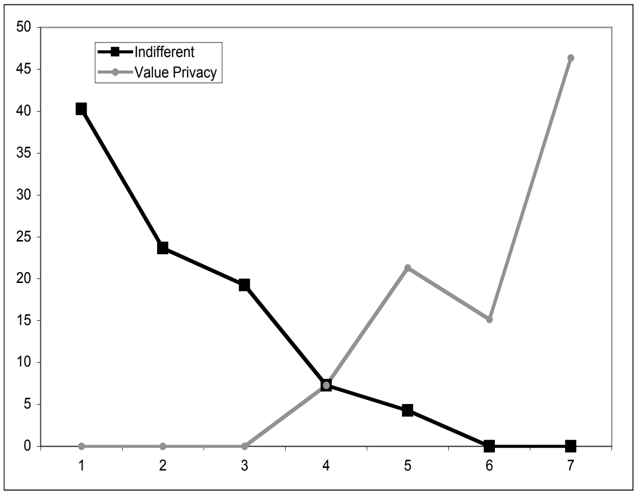

Figure 3. Impact of personal disposition towards privacy.

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 4). Misunderstanding of technology seemed to create a false sense of security leading to lower concern for privacy ($p \sim 0.001$), whereas correct understanding exposed risks, and thus raised privacy concern. For example, one 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*".

[1] Percentages add to greater than 100% since several responses contained multiple justifications.

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*".

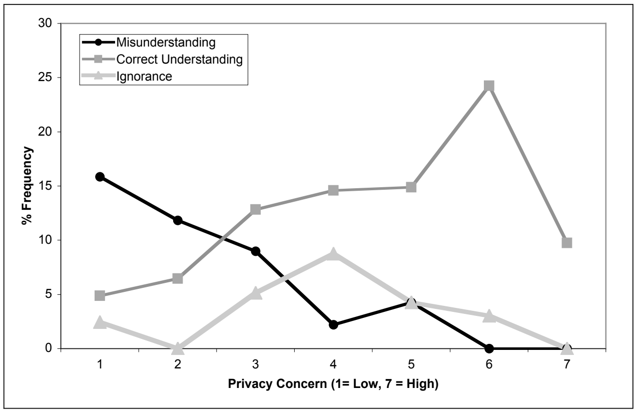

Figure 4. Impact of technological understanding.

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 4, where the line indicating "ignorance" peaks at the middle and falls away on both sides. This is also reflected in justifications such as, "*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). The mean (mean: 3.77, median: 4, mode: 4, sd: 1.8) was, in fact, slightly higher (p ~ 0) 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%)[2] were also factors considered important by respondents[3].

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). 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.

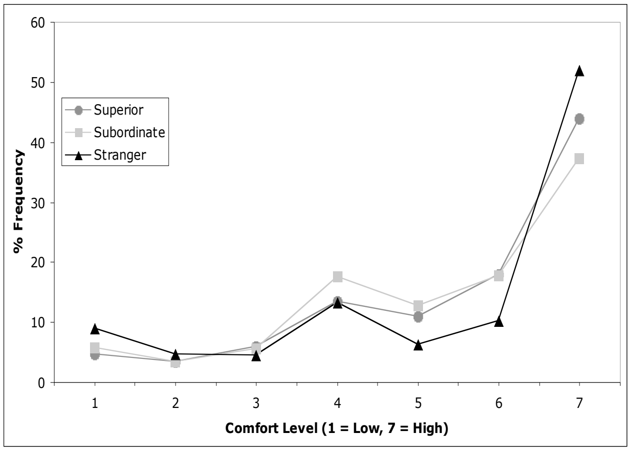

Figure 5. Privacy attitudes towards superiors, subordinates & strangers are quite similar.

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). 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 5). Given the high level of privacy one typically desires from strangers, this corroborates the finding of Lederer et. al. [5] that hierarchical relationships may involve higher privacy tensions.

While our preliminary analyses indicate no significant effects of demographics except age (privacy concern increases with age, p ~ 0.003), we are still investigating effects of factors such as employment, education and marital status.

4. IMPLICATIONS

Our findings make a case for demystifying the technology underlying an IM system in order to promote better risk assessment through increased technological awareness. For instance, while it is certainly unreasonable to expect that the average user will understand how encryption works [9], it is fairly easy to communicate that an unencrypted conversation can potentially be read by third-parties. This could be achieved via a simple warning not to disclose sensitive information without encryption. The effectiveness of the simple "padlock" icon in Web browsers needs to be emulated; it promotes just enough technological awareness without burdening the user with unnecessary detail.

Respondent concerns regarding archiving or logging indicate a perceived lack of control over persistence of conversations. In fact, in many cases this led to self-censorship of what was said. For instance, one respondent commented, "*I know that most*

[2] This includes IM contacts as well as those in the vicinity of the computer.

[3] Again, percentages add to greater than 100% since several responses contained multiple justifications.

people do log their IM conversations, so I try and keep that in mind while talking privately with someone about sensitive things." To alleviate these concerns, particularly for more sensitive conversations, more balanced control over archiving needs to be designed (for example, requiring permission of all parties for saving a conversation).

Despite the wide range of responses for privacy concern, we found that, similar to Westin's [8] classification of consumer privacy attitudes, a three-level low (1-3), medium (4) and high (5-7) grouping was just as effective in discerning the privacy attitudes of users. This could be utilized to reduce the burden of extensive privacy management by providing suitable templates for low, medium and high levels of desired privacy (akin to settings in some Web browsers).

The differences in privacy attitudes towards various categories of contacts suggest that contact grouping in IM could be extended to improve effectiveness of privacy management. Currently, most privacy settings in IM applications apply globally to all contacts, resulting in insufficient support for more discriminatory privacy control. We propose providing the ability to configure privacy settings separately for each user-specified group of IM contacts. At first glance, this may appear rather burdensome. However, the burden could be alleviated in a variety of ways – inheritance from global defaults, templates of settings for commonly encountered groups, and gradual evolution of settings by presenting configuration options in appropriate contexts.

Finally, the fact that privacy conscious users are more likely to change default settings seems to suggest that IM systems have lower privacy protection by default. We advocate system defaults be set to offer the highest practical level of privacy protection. Changing privacy protection by the system from an opt-in to an opt-out model seems more useful as it makes the choice to give up privacy a deliberate user action rather than the default selection.

5. CONCLUSION

Our analysis of privacy attitudes in IM revealed a broad spectrum of user attitudes and practices. We discussed several factors that contribute to privacy concerns, or lack thereof. The impact of technological understanding is quite noteworthy. In particular, those who exhibit an inaccurate understanding of technology are led to assume that they have more privacy protection than actual level of protection present. This underscores the need for building interfaces that make the underlying technology of IM systems more transparent to the average user, especially in an era where rampant increase in spam, spyware, malware and viruses is contributing to considerable user confusion [1]. Given the observed differences in user expectations for various categories of contacts, we believe that contact-grouping functionality in IM needs to be extended to allow different privacy configurations for different groups. Finally, since "content" forms a significant aspect of user privacy concerns, giving users more control over archiving may be the key for preventing users from shunning IM for sensitive conversations.

6. ACKNOWLEDGMENTS

We would like to thank Heather Pulliam, Mihir Mahajan, Jennifer Rode, and all of interviewees.

7. REFERENCES

[1] Dourish, P., and Anderson, K. *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, 2005.

[2] Grinter, R.E., and Palen, L., Instant Messaging in Teen Life. In *Proceedings of the 2002 ACM Conference on Computer Supported Cooperative Work* (New Orleans, LA, USA, 2002). ACM Press, New York, NY, USA, 21-30.

[3] Herbsleb, J.D., Atkins, D.L., Boyer, D.G., Handel, M., and Finholt, T.A., Introducing Instant Messaging and Chat in the Workplace. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Minneapolis, MN, USA, 2002). ACM Press, New York, NY, USA, 171-178.

[4] Isaacs, E., Walendowski, A., Whittaker, S., Schiano, D.J., and Kamm, C., The Character, Functions, and Styles of Instant Messaging in the Workplace. In *Proceedings of the 2002 ACM Conference on Computer Supported Cooperative Work* (New Orleans, LA, USA, 2002). ACM Press, New York, NY, USA, 11-20.

[5] Lederer, S., Mankoff, J., and Dey, A.K., Who Wants to Know What When? Privacy Preference Determinants in Ubiquitous Computing. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Ft. Lauderdale, FL, USA, 2003). ACM Press, New York, NY, USA, 724-725.

[6] Muller, M.J., Raven, M.E., Kogan, S., Millen, D.R., and Carey, K., Introducing Chat into Business Organizations: Toward An Instant Messaging Maturity Model. In *Proceedings of the 2003 International ACM SIGGROUP Conference on Supporting Group Work* (Sanibel Island, FL, USA, 2003). ACM Press, New York, NY, USA, 50-57.

[7] Patil, S., and Kobsa, A., Instant Messaging and Privacy. In *Proceedings of Human Computer Interaction 2004* (Leeds, UK, 2004). 85-88.

[8] Westin, A. *Harris-Equifax Consumer Privacy Survey*. Atlanta, GA, USA, 1991.

[9] Whitten, A., and Tygar, J.D., Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *Proceedings of the 8th USENIX Security Symposium* (Washington, D.C., USA, 1999). 169–184.