Interacting with Computers 22 (2010) 206–217

Contents lists available at ScienceDirect

Interacting with Computers

journal homepage: www.elsevier.com/locate/intcom

Enhancing privacy management support in instant messaging

Sameer Patil *, Alfred Kobsa

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

ARTICLE INFO

Article history:
Received 26 February 2008
Received in revised form 20 October 2009
Accepted 24 October 2009
Available online 1 November 2009

Keywords:
Privacy
Instant Messaging, IM
Privacy management
Impression management
Computer-supported communication
Computer supported collaborative work, CSCW

ABSTRACT

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

1. Introduction

Instant Messaging (IM) was popularized by adolescents but today it is used by people of all ages. While its initial focus was on supporting social ties among friends, it is increasingly being adopted as a tool for collaborative work due the utility of its awareness and communication mechanisms (Herbsleb et al., 2002). Consequently, IM use is no longer limited to the home but has expanded to include workplaces and educational institutions.

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

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

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

The goal of our work is to analyze privacy attitudes and practices of IM users and enhance the "privacy friendliness" of IM in order to boost its utility, particularly for collaborative work. To

* Corresponding author. Address: Department of Informatics, Donald Bren School of Information and Computer Sciences, University of California, Irvine, Irvine CA 92697-3440, USA. Tel.: +1 949 258 3474; fax: +1 949 824 1715.
E-mail addresses: patil@uci.edu (S. Patil), kobsa@uci.edu (A. Kobsa).

0953-5438/$ - see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.intcom.2009.10.002

achieve this objective, we investigated the nature of privacy concerns among IM users along with the various factors that influence these concerns and used the insights from these studies to design various enhancements to IM privacy management. This paper describes a fully functioning prototype that implements these designs. We also describe the results of a user study conducted to evaluate the usability as well as the anticipated utility of the different privacy-enhancing features that the prototype provides.

2. Related work

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

2.1. User studies of awareness systems

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

Palen (1999) found that socio-technical mechanisms controlled privacy even in highly open network calendaring environments. Users managed privacy partly via technical access control, partly via the norm of reciprocity,[1] partly via practices such as cryptic entries, omissions, defensive scheduling, and partly via social anonymity within the organizational context. The system we describe in the paper follows such a socio-technical approach, relying on both social and technical control and enforcement.

Later studies of awareness systems began to target privacy as the primary object of investigation (Adams, 1999; Adams and Sasse, 1999; Consolvo et al., 2005; Lederer et al., 2004; Olson and Teasley, 1996). These studies identified that the relationship with the information recipient, the purpose or usage of information, the context, and the sensitivity of content are important factors in making privacy judgments.[2] In studies specific to IM, Herbsleb et al. (2002) found that the lack of lightweight mechanisms to address privacy is a barrier for setup and adoption. Grinter and Palen (2002) illustrate (albeit with teenagers) that users adapt system capabilities to their own ends. Teens in their study made enterprising use of access permissions, profiles, status messages, and screen names to manage privacy. Nardi et al. (2000) found that plausible deniability of presence is used for managing privacy in instant messaging.

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

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

2.2. Theories, principles, and guidelines

Privacy is recognized to be a nuanced and situated concept without a universal definition. The rich body of literature on privacy in the social sciences is testimony to its intricate connections with the broader social context (Dourish and Anderson, 2005). Due to this complexity, technology designers have found it difficult to analyze and frame the privacy issues unveiled by user studies. Researchers have tried to address this problem by attempting to articulate theoretical insights regarding privacy in forms that are more accessible to system designers. For instance, Boyle et al. (2000) describe a vocabulary of privacy that designers can employ for an unambiguous discussion of privacy issues. To suggest ways of thinking about privacy in socio-technical environments, Palen and Dourish (2003) outline a model of privacy that is based on the theory of social psychologist Irwin Altman. It views privacy as a process that regulates the boundaries of disclosure, identity and temporality. This process is both dynamic (i.e., shaped by personal and collective experiences and expectations) and dialectic (i.e., under continuous boundary negotiation).

Researchers also compiled various privacy-related findings from user studies into design principles and guidelines in order to allow for better privacy management. Bellotti and Sellen (1993) propose a design framework based on feedback and control regarding information capture, construction, accessibility, and purpose. The purpose of feedback mechanisms is to provide users with information that helps them make judgments regarding privacy, while the purpose of control is to empower them to take appropriate actions to manage privacy. Langheinrich (2001) draws upon Fair Information Practices (Landesberg et al., 1998) and proposes that privacy-sensitive systems ought to notify their users appropriately, seek user consent, provide choice, allow for user anonymity or pseudonymity, limit scope with proximity and locality, ensure adequate security, and implement appropriate information access. Iachello and Abowd (2005) provide an additional principle of proportionality ("*any application, system tool, or process should balance its utility with the rights to privacy of the involved individuals*"). In contrast, Lederer et al. (2004) outline five pitfalls: obscuring potential information flow, obscuring actual information flow, emphasizing configuration over action, lacking coarse-grained control, and inhibiting existing practice. Hong et al. (2004) describe privacy risk models to analyze how well a system meets such principles or avoids pitfalls. These risk models are a set of questions on information sharing, pertaining to the social and organizational context in which the system is situated, and to the technology which is used to implement the system. To incorporate user perceptions, Adams (1999) provide a privacy model based on information sensitivity, information receiver, and information usage, in which each of the three factors interacts with the others. As the following sections will illustrate, our design draws on many of these interrelated principles and guidelines.

2.3. Design techniques and approaches

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

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