Privacy as Impression Management

Sameer Patil, Alfred Kobsa
Institute for Software Research (ISR)
School of Information and Computer Science
University of California, Irvine
Irvine, CA 92697 USA
{patil, kobsa}@uci.edu

ISR Technical Report #UCI-ISR-03-13
December 2003

ABSTRACT

In this paper, we suggest that the primary concern regarding privacy in collaborative work settings is "*impression management*". We discuss a host of factors which influence privacy management in such settings. Finally, we offer some suggestions regarding how designers can empower users to manage their impression.

Keywords: Privacy, Collaboration, Impression Management, Instant Messaging.

This research has been supported by the National Science Foundation (grant #0205724).

Privacy as Impression Management

Sameer Patil, Alfred Kobsa
Institute for Software Research (ISR)
School of Information and Computer Science
University of California, Irvine
Irvine, CA 92697 USA
{patil, kobsa}@uci.edu

ISR Technical Report #UCI-ISR-03-13
December 2003

ABSTRACT
In this paper, we suggest that the primary concern regarding privacy in collaborative work settings is "*impression management*". We discuss a host of factors which influence privacy management in such settings. Finally, we offer some suggestions regarding how designers can empower users to manage their impression.

Keywords
Privacy, Collaboration, Impression Management, Instant Messaging.

INTRODUCTION
There is an inherent tension between privacy and awareness in the context of collaborative work - particularly in case of geographically distributed work teams. Timely information about current activities, work progress and availability of other team members is very valuable for fostering informal communication among team members and for the low-level synchronization of work activities (Dourish & Bellotti, 1992; Herbsleb et. al., 2000). Yet, people are usually quite reluctant to agree to an unlimited surveillance and disclosure of their whereabouts and activities (Want et. al., 1992). We aim to identify central factors that must be considered in the analysis of this tension between workgroup awareness and individual privacy, and use this analysis to provide software mechanisms to assist distributed work teams in negotiating solutions to the tension.

COMPARISON OF INSTANT MESSAGING SYSTEMS
Our comparison of popular instant messaging (IM) systems (Patil & Kobsa, 2003) illustrates how even a conceptually simple collaborative computing system such as IM can be quite complicated when analyzed from the point of view of privacy. We have collected the following principles and factors which seem to influence privacy management:

Reciprocity
Reciprocity ensures that an individual can only request information about others that he or she is willing to disclose about himself or herself, and vice versa.

Feedback
Feedback involves providing individuals with information that suitably tells them what information about them is being accessed by whom, in which form and at what time.

Context
Which information should be made available to whom and in which form is highly context dependent and keeps changing continually.

Control
Ideally, all information should be under the control of the respective individual(s) involved. This allows the individual(s) to specify how, when and to whom, the information may be revealed.

Norms
Norms regarding privacy can have diverse origins. They may stem from shared cultural understandings, may evolve with growing organizational memory, may have been set through explicit policies or mandates, or a combination of of such influences.

Inference
People manage privacy at the micro level, focusing on the particular task or issue at hand, and on the current context. However, several such pieces of micro-information could be collected together to form a macro-level awareness that reveals information that people may not have wanted to divulge intentionally. For example, an individual may only wish to reveal on his or her shared calendar that he or she is in a meeting in the conference room without specifying the participants. However, if other participants of the meeting also maintain shared calendars, then looking up the various personal calendars may reveal who the participants of the

This research has been supported by the National Science Foundation (grant #0205724).

meeting are – something which some or all of the participants may have wished not to divulge.

Overhead

Managing privacy involves overhead in terms of performing tasks which are unrelated to the primary work (e.g. remembering to set IM status to "busy"). These secondary tasks may be time consuming, tedious and/or distracting.

Incentives

Individual and/or group motivations influence how people may manage their privacy. Individuals may be willing to sacrifice privacy if they receive sufficient benefits. Moreover, the "overhead" required in privacy management needs to be balanced with the direct benefits for the individual for these efforts (Grudin, 1988).

Conflicts

People's desires, opinions and expectations regarding privacy may conflict with each other. Consider, for example, two colleagues who share an office, one of whom prefers the office door to be kept shut while the other prefers to leave it open.

Archiving

Archiving of information in any form – paper, digital, organizational memory etc. – conserves it over time. As a result, such information may later be available out of context, in a manner different from the way in which it was originally meant to be utilized, and to people other than those to whom it was addressed.

We advocate that the above factors be analyzed for every collaborative computing system. A solid understanding of these issues can aid in designing features and mechanisms to address privacy effectively.

PRIVACY AS IMPRESSION MANAGEMENT

"Privacy" seems to serve different aims in different contexts. For instance, in the context of e-commerce (Teltzrow & Kobsa, 2004), privacy aims at protecting personal data of individuals from organizations that may be in a position to use this data in a potentially harmful manner. In field studies with different organizations, Dourish et al. (2003) identified a keen interest of computer users to protect themselves from hackers, stalkers, spammers and marketers.

We claim that in the context of group collaboration, an important driving force behind individual desire for privacy is the wish to control one's impression from the point of view of others (more specifically team members and superiors). This factor is likely to strongly influence the point of balance between demands for privacy and the consent to disclose awareness information. An individual is likely to demand more privacy in matters which could potentially reflect poorly upon himself or herself. On the other hand, he or she may tolerate, or even demand, less privacy when the situation creates a favorable impression of him or her. For example, due to a general fear of monitoring, employees may be reluctant to distribute records of the exact time at which they arrive at work every day. However, an employee who consistently comes in early may in fact wish to have this fact known widely as a reflection of greater commitment toward work. In addition, the kind of impression one wants to present to others is dependent on the kind of relationship one has with them. Providing information to trusted colleagues will likely raise fewer privacy concerns than to superiors or unknown third parties.

Thus, a privacy-sensitive group collaboration system should ideally allow its users to seamlessly manage their "impression" as seen by each of the various parties involved. It ought to give users the opportunity to inspect the various pieces of information about themselves that can be viewed by others, and also to obtain summaries and statistics about it.[1] Users could also be provided with the capability to receive timely alerts and notifications regarding changes to various factors and parameters that are of particular importance to them.

IMPLICATIONS FOR DESIGN

In designing collaborative computing systems with impression management mechanisms, we suggest paying particular attention to three major factors:

Defaults

Given the complex, fuzzy and context-dependent nature of privacy, the number of options and settings that need to be managed is quite complicated. As a result, designers must provide defaults which are widely applicable across persons and situations. Moreover, given that users rarely change the defaults, it is all the more important to get as many defaults right as possible. The values of defaults ought to be informed by detailed studies of the people, the task(s) and the setting(s) in which the system operates.

Modifiable policies

Since the notion of privacy is highly nuanced, it is impossible to devise universally applicable policies. For example, a system may have the policy of not revealing one's home phone number to anyone except one's family and personal friends. However, in case of an emergency, one is unlikely to expect a rigid enforcement of such a policy. Designers need to be careful to avoid setting rigid policies which cannot be modified.

Interface and Interaction

Finally, a great deal of attention needs to be paid to the user interface and interaction. Feedback regarding how one's impression is being managed should be provided in a context-sensitive, non-intrusive and seamless manner. Interaction with the user should be designed so that specifying and modifying one's status, settings, and policies, requires the least possible overhead in terms of time and effort.

[1] We recommend against providing such summaries and statistics of awareness information about others, in order not to facilitate surveillance.

CONCLUSION

The great promise of technologies for collaborative work that increase group awareness is often overshadowed by the accompanying privacy concerns, which are inherent to such systems. In systems devised for communication and collaboration, the privacy concerns in question are mainly with respect to other individuals one interacts with – such as colleagues, superiors, subordinates, friends and family – as opposed to big, nameless entities such as corporations and governments. We suggest that the primary concern regarding privacy in collaborative work settings is managing one's impression upon others. We believe that focusing on the interface, and providing modifiable policies and settings (with suitable defaults and seamless interaction), can allow designers of collaboration systems to empower users to appropriately manage their impression toward other concerned parties.

ACKNOWLEDGMENTS

We wish to thank Paul Dourish and Max Teltzrow for thoughtful discussions which have contributed to some of the ideas in this paper.

REFERENCES

1. Dourish, P. and V. Bellotti (1992) Awareness and Coordination in Shared Workspaces. In *Proceedings of The ACM conference on Computer-Supported Cooperative Work*, Toronto, Ontario, Canada, ACM Press, New York, NY, USA.
2. Dourish, P., Grinter, R. E., Dalal, B., Delgado de la Flor, J. and M. Joseph (2003) Security Day-to-Day: User Strategies for Managing Security as an Everyday, Practical Problem. University of California, Irvine, Institute for Software Research, Technical Report #UCI-ISR-03-5 (http://www.isr.uci.edu/tech_reports/UCI-ISR-03-5.pdf).
3. Grudin, J. (1988) Why CSCW Applications Fail: Problems in the Design and Evaluation of Organizational Interfaces. In *Proceedings of The ACM Conference on Computer-Supported Cooperative Work*, Portland, Oregon, USA, ACM Press, New York, NY, USA.
4. Herbsleb, J. D., Mockus A., Finholt, T. A., and R. E. Grinter (2000) Distance, Dependencies, and Delay in a Global Collaboration. In *Proceedings of The ACM Conference on Computer Supported Cooperative Work*, Philadelphia, Pennsylvania, USA, ACM Press, New York, NY, USA.
5. Patil S., and A. Kobsa (2003) The Challenges to Preserving Privacy in Awareness Systems. University of California, Irvine, Institute for Software Research, Technical Report #UCI-ISR-03-3 (http://www.isr.uci.edu/tech_reports/UCI-ISR-03-3.pdf).
6. Teltzrow, M. and A. Kobsa (2004) Impacts of User Privacy Preferences on Personalized Systems – a Comparative Study. In *Designing Personalized User Experiences for eCommerce*, C. M. Karat, J. Blom and J. Karat (eds.), Dordrecht, Netherlands, Kluwer Academic Publishers.
7. Want, R., Hopper, A., Falco, V. and J. Gibbons (1992) The Active Badge Location System. *ACM Transactions on Information Systems (TOIS)* **10**(1): pp. 91-102.