Designing with Privacy in Mind

Sameer Patil, Alfred Kobsa
Department of Informatics
University of California, Irvine CA 92697 USA
{patil, kobsa}@uci.edu

INTRODUCTION

Designers and researchers of awareness systems have recognized and acknowledged the existence of privacy concerns in systems covering a wide variety of domains (e.g. email [e.g., 1], media spaces [e.g., 7], data mining [e.g. 18], homes with advanced domestic technologies [e.g., 8] and so on). Several factors contribute to making dealing with privacy issues in the digital domain quite challenging [13]. However, designing effective solutions to address these concerns is imperative to ensure that benefits that could be derived from an awareness system are not lost due to underuse, or abandonment [5, 19].

A major part of the problem seems to be that privacy management features of the system do not form a central concern for designers. Privacy is treated as a secondary aspect, and gets secondary treatment. As a result, mechanisms for privacy management may only be added as an afterthought, or sometimes not at all, leaving them as open issues for future work.

In the following section, we describe some of our work in studying privacy issues in awareness systems. Our experiences have led us to believe that it is only when designers keep privacy in mind right from the outset that awareness systems can provide adequate and effective mechanisms for dealing with privacy issues, and can empower users to control these aspects as appropriate. Such an approach will also minimize the chances of running into unanticipated privacy problems upon system deployment.

PRIVACY CONSIDERATIONS IN VARIOUS AWARENESS SYSTEMS

Over the past couple of years, we have been involved with privacy research involving a number of awareness systems.

Instant Messaging (IM)

In the past few years, IM has been steadily gaining popularity in the workplace as a useful awareness mechanism and communication tool. The 2004 Pew Internet & American Life surveys reveal that 11 million Americans use IM at work and they are becoming fond of its capacity to encourage productivity and interoffice cooperation [17]. International Data Corporation (IDC) forecasts 200 million corporate IM users worldwide by 2006. While it had been found that IM users harbor privacy concerns [4], we did not find any systematic investigation of these concerns.

To fill this gap, we started by conducting semi-structure interviews with frequent users of IM [14]. We discovered that privacy concerns in IM seemed to be related to three main dimensions – who (contacts), when & where (availability), and what (contents). To deal with these issues, users employed some combination of self-governance, carefully evolved practices (self, group, or social), mandated or mutually agreed-upon policies and guidelines, and software settings (e.g. blocking contacts, or setting one's status to "invisible").

To dig deeper into these issues, we administered a large online survey developed based on findings from the interviews [12]. On a 7-point Likert scale, the reported concern about IM privacy spanned the whole range from very low to very high, with the average being slightly below "medium". Respondents' justifications for their privacy concerns, or lack thereof, revealed that the main contributing factors were: sensitivity of content, personal disposition towards privacy, understanding of technology, and potential persistence of conversations via archiving or logging.

The impact of technological understanding is quite noteworthy. Misunderstanding of technology seemed to create a false sense of security leading to lower concern for privacy, 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*". In contrast, another respondent who had an accurate understanding of technology was highly concerned (6) and remarked, "*All text is in the clear. Public IM services can store the text that I send, corporate (internal) services can do likewise and also monitor my availability*". Self-proclaimed ignorance towards technology appeared to make users ambivalent (57% of those who said they were ignorant about technology indicated their level of privacy concern as 4, and 86% were between 3-5). This is reflected in justifications such as, "*It's not entirely clear to me how secure a conversation is on IM*". This underscores the need for building interfaces that make the underlying technology of IM systems more transparent to the lay user, especially in an era where rampant increase in spam, spyware, viruses etc. is contributing to considerable user confusion.

Expectations regarding privacy for various categories of contacts differed significantly. In general, friends and significant others were trusted much more than the other groups. Interestingly, there was no statistical difference in terms of desired privacy level between superiors and strangers, or between subordinates and strangers. Given the high level of privacy desired from strangers, this indicates that hierarchical relationships between people may involve higher privacy tensions than others.

We noted that an increased concern for privacy leads to increased 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.

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 [20], it is fairly easy to communicate that an unencrypted conversation can potentially be read by unintended recipients. This could be achieved via a simple warning not to disclose sensitive information without encryption. The success of the simple "padlock" icon in Web browsers needs to be emulated; it promotes just enough technological awareness without burdening the user with extraneous details.

Respondent concerns regarding archiving or logging indicate a perceived lack of control over the persistence of their conversations. In fact, in many cases this leads to self-censorship of what is said. For instance, one respondent commented, "*I know that most 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 symmetric 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 a three-level low (1-3), medium (4) and high (5-7) grouping is just as effective in discerning the privacy attitudes and practices of users. This could be utilized to reduce the burden of extensive privacy management by providing relevant templates for low, medium and high levels of desired privacy (akin to settings in some Web browsers).

Finally, the fact that the privacy conscious are more likely to change default settings seems to suggest that IM systems have lower privacy protection by default. We advocate that system defaults be set to offer the highest practical level of privacy protection. Changing user 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 vice versa.

MySpace

MySpace is an interactive visualization of the physical workplace that provides dynamic information about people, places and equipment. Using mySpace, we conducted a study (N=36) of user preferences for balancing awareness with privacy [15]. Participants defined permissions for sharing of location, availability, calendar information and IM activity within mySpace deployed at a large technology company.

Participants exhibited a strong preference for managing privacy at the group level with 25 out of 36 choosing the "Groups" mode for configuring permissions. Defining permissions at the group level appears to provide the flexibility needed to appropriately manage the balance between awareness and privacy, without undue burden. Based on these findings, we argue for providing grouping functionality in awareness systems for more than contact list organization. Configuration burden could be further reduced by providing templates of settings for commonly used groups such as Team, Collaborators, or Family. Defaults for templates could be based on a quick user study of the target population (or on our findings if working in a similar environment).

We discovered that "family" received high levels of awareness sharing. Interestingly, "team" was granted comparable levels during business hours at work. In particular, system builders of location-aware systems will be heartened that, although location was treated as the most sensitive aspect of awareness, during working hours users were not averse to sharing their location with colleagues considered to be part of their team. The mode of permission for team members during business hours was the highest possible setting (i.e. room-level location). This seems to suggest that empowering users to control how and when aspects of their context are shared with whom, can enable them to find more suitable points of balance between awareness and privacy. If designers provide greater user control over more sensitive aspects of awareness, users may feel comfortable enough to appropriately share such information via the system.

Surprisingly, presenting participants with a detailed list of all pieces of personal context to which the system had access, did not seem to scare users into choosing more privacy-conservative settings. In fact, it appeared as if such a disclosure may act as a trust-builder, reassuring users to reveal more information to the colleagues on their team [10]. We encourage designers to strive for increased system transparency to build trust. In addition, appropriate feedback mechanisms and interfaces need to also be explored to further help users visualize their permission settings.

Blogs

Blogs have recently been gaining a lot of attention from the media. At the same time, researchers and system designers have begun exploring the potential of blogs for supporting collaboration. A few companies (e.g. Microsoft) are actively promoting both personal and collective blogs as a useful communication and awareness tool for more effective collaboration. However, apart from isolated stories in the media [16], relatively little research has been done regarding privacy considerations surroundings blogs as a system, and blogging as a practice. We conducted extensive, semi-structured interviews with 16 bloggers from the "Slash" community. Slash is a genre of fan-fiction that focuses on same-sex relationships between characters. We are still in the process of analyzing the data. However, preliminary analysis has revealed several insights regarding privacy practices employed by "slashers" – both while writing to their own blog, and while leaving comments on the blogs of others. Some of the privacy-protecting strategies slashers use include deliberate and careful separation of slash identity from other identity or identities (offline and/or online), "friends-locking" of posts or comments to limit audience, self-censorship of content, maintenance of multiple slash identities and hierarchical organization of the "friends list".

Privacy and Identity Management for Europe (PRIME)

PRIME (http://www.prime-project.eu.org/) addresses research issues of digital identity management and privacy in the information society. We have started a collaboration with PRIME with the aim of complementing their research with the North American perspective. side. In particular, we plan to investigate how cultural and legal differences might manifest themselves in privacy aspects. Currently, we are comparing and contrasting results from various privacy surveys administered to European and North American populations. Later this year, we will be conducting analogous privacy experiments in Europe and North America.

DISCUSSION

Based upon our work coupled with relevant existing literature, we discuss below some of the factors that we believe may contribute to the inadequate attention by system designers to privacy.

Privacy is difficult to grasp:

Privacy is a concept that has escaped a precise definition due to its highly nuanced and context-dependent nature. This makes dealing with privacy issues quite challenging. This is all the more true in awareness systems which increasingly need to span countries and cultures [9].

Privacy protection a secondary function:

Awareness, not privacy, is the focus of attention of an awareness system. Analogous to security, protecting privacy is not the primary function of the system, and as a result receives secondary attention. In fact, privacy may even be viewed as a nuisance that gets in the way of the awareness aspects of the system.

Privacy mechanisms lack clear design guidelines:

Apart from a couple of notable attempts [2, 6], there is relatively little guidance for designers regarding best practices to follow and pitfalls to avoid. The insights gained from both theory [3, 11] and empirical studies [e.g., 5, 7, 15, 19] need to be converted into concrete design suggestions applied to specific domains.

Understanding privacy aspects requires end-user involvement:

Given the highly personal nature of privacy, there are likely to be mismatches in the perspectives on privacy of the designers and the end users. As a result, designing effective privacy mechanisms requires involving end-users in some form – as subjects in an empirical investigation, participatory designers, alpha/beta testers etc. This may not always be practically feasible due to time, budget, and access constraints.

Privacy features need iterative improvement:

Despite careful attention, it is always possible that unanticipated privacy issues crop up after system deployment [5, 19]. Moreover, organizational, technological changes and increase in user proficiency can contribute to changes in expectations and practices regarding privacy. Inability to adapt to such changes could undermine long term success of the system. Such evaluations are typically expensive and lengthy. Further, empirical studies of privacy pose their own methodological challenges.

SUGGESTED APPROACHES

Various approaches could be used to address the problems outlined in the previous section. Some of these – deriving guidelines from theory, qualitative and quantitative empirical studies of users and the domain, participatory design, iterative improvement – have already been alluded to in the previous section.

However, merely providing mechanisms to empower users to adequately and efficiently control privacy is not enough. In addition, we argue that privacy management features need to provide default settings that are an acceptable starting point for most individuals in order to avoid the pitfall of requiring too much configuration [6]. Since majority of users rarely modify default settings, getting defaults right could ensure a balanced privacy-awareness setting from the outset. Even if only 75-80% of the defaults are appropriately set, the user is perhaps more likely to fine-tune the rest. Setting defaults to broadcast more awareness information than necessary can undermine individual privacy, and may lead to underutilization (or even abandonment) of the system. On the other hand, creating defaults with higher privacy settings than required could undermine the awareness benefits of the system.

In conclusion, the tension between awareness and privacy will always exist. Only by designing awareness systems with privacy in mind from the outset, designers can hope to empower users to effectively, efficiently and seamlessly achieve an appropriately comfortable point of balance between awareness and privacy.

WORKSHOP RELEVANCE

We believe that these findings and ideas will stimulate discussion and debate regarding privacy aspects of awareness systems from both researchers and practitioners. The feedback and critique from the workshop will no doubt help us refine our ideas, and possibly suggest new avenues for exploration. We also hope to explore opportunities for collaboration with the industry, in particular regarding studying privacy issues "in the field".

ACKNOWLEDGMENTS

We wish to thank our collaborators, Jennifer Lai and Steve Abrams, in the various projects described. We also acknowledge Paul Dourish, and Jennifer Rode for numerous discussions that have contributed to shaping some of these ideas.

REFERENCES

1. Bellotti, V. (1996) What You Don't Know Can Hurt You: Privacy in Collaborative Computing, In Proc. HCI Conference on People and Computers XI.
2. Bellotti, V., and Sellen, A., (1993) Design for Privacy in Ubiquitous Computing Environments, In Proc. ECSCW 1993, pp. 75-90.
3. Goffman, E., (1959) The Presentation of Self in Everyday Life, Doubleday, Garden City, NY.
4. Grinter, R. E., and Palen, L. (2002) Instant Messaging in Teen Life, In Proc. CSCW 2002, pp. 21-30.
5. 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 Proc. CHI 2002, pp. 171-178.
6. Lederer, S, Hong, J. I., Dey, A. K., and Landay, J. A. (2004) Personal Privacy through Understanding and Action: Five Pitfalls for Designers, Personal and Ubiquitous Computing, 8 (6), pp. 440-454.
7. 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 Proc. CHI 1991, pp. 203-208.
8. Meyer, S., and Rakotonirainy, A. (2003) A Survey of Research on Context-aware Homes, In Proc. Australasian Information Security Workshop Conference on ACSW Frontiers, pp. 159-168.
9. Milberg, S. J., Burke, S. J., Smith, H. J., and Kallman, E. A. (1995) Values, Personal Information Privacy, and Regulatory Approaches, Communications of the ACM, 38 (12), pp. 65-74.
10. Moore, D. A., Kurtzberg, T. R., Thompson, L. L., and Morris, M. W. (1999) Long and Short Routes to Success in Electronically Mediated Negotiations: Group Affiliations and Good Vibrations, Organizational Behavior and Human Decision Processes, 77 (1), pp. 22-43.
11. Palen, L., and Dourish, P. (2003) Unpacking "Privacy" for a Networked World, In Proc. CHI 2003, pp. 129-136.
12. Patil, S., and Kobsa, A. (2005) Uncovering Privacy Attitudes and Practices in Instant Messaging, Submitted to CHI 2005, (under review).
13. Patil, S., and Kobsa, A. (2004) Preserving Privacy in Awareness Systems, In Wissen in Aktion, R. Hammwöhner, M. Rittberger and W. Semar (eds.), University of Konstanz Press, Konstanz, Germany, pp. 119-129.
14. Patil, S., and Kobsa, A. (2004) Instant Messaging and Privacy, In Proc. HCI 2004, Leeds, U.K.
15. Patil, S., and Lai, J. (2005) Who Gets to Know What When: Configuring Privacy Preferences in an Awareness Application, In Proc. CHI 2005 (to appear).
16. Rosen, J. (2004) Your Blog or Mine?, New York Times, December 19, 2004.
17. Shiu, E., and Lenhart, A. (2004) How Americans Use Instant Messaging, Pew Internet & American Life Report.
18. Thuraisingham, B. (2002) Data Mining, National Security, Privacy and Civil Liberties, ACM SIGKDD Explorations Newsletter, 4 (2), pp. 1-5.
19. Want, R., Hopper, A., Falcão V., and Gibbons, J. (1992) The Active Badge Location System, ACM Transactions on Information Systems, 10(1), pp. 91-102.
20. Whitten, A. and Tygar, J. D. (1999) Why Johny Can't Encrypt: A Usability Evaluation of PGP 5.0, In Proc. Usenix Security Symposium, pp. 169-184.