ISR Institute for Software Research
University of California, Irvine

The Challenges in Preserving Privacy in Awareness Systems

Sameer Patil
Univ. of California, Irvine
patil@ics.uci.edu

Alfred Kobsa
Univ. of California, Irvine
kobsa@ics.uci.edu

April 2003

ISR Technical Report # UCI-ISR-03-3

Institute for Software Research
ICS2 210
University of California, Irvine
Irvine, CA 92697-3425
www.isr.uci.edu

www.isr.uci.edu/tech-reports.html

The Challenges in Preserving Privacy in Awareness Systems

Sameer Patil, Alfred Kobsa

Institute for Software Research,
University of California, Irvine
Irvine, CA 92697-3425, USA
{patil, kobsa}@uci.edu

ISR Technical Report # UCI-ISR-03-3

April 2003

Abstract: Awareness of the activities of one's co-workers is valuable for effective collaboration. The need for awareness is however frequently in conflict with privacy concerns of the people involved. This paper discusses various factors and principles that influence and inform a privacy-preserving design of awareness systems.

The Challenges in Preserving Privacy in Awareness Systems

Sameer Patil, Alfred Kobsa
School of Information and Computer Science
University of California, Irvine
Irvine, CA 92697-3425, USA
{patil, kobsa}@uci.edu

ISR Technical Report # UCI-ISR-03-3
April 2003

Abstract

Awareness of the activities of one's co-workers is valuable for effective collaboration. The need for awareness is however frequently in conflict with privacy concerns of the people involved. This paper discusses various factors and principles that influence and inform a privacy-preserving design of awareness systems.

Keywords: *Privacy, Awareness, Distributed software development, CSCW, Instant messaging*

1. Awareness

Awareness of the activities of collaborators helps individuals plan, orient and coordinate their own work to fit in with the larger scheme of things, with respect to the team, department or organization, thereby increasing efficiency and effectiveness of individual work as well as the work that is carried out collaboratively (Dourish and Bellotti 1992). It is no surprise then that the more tightly-coupled the collaborative activity, the higher the amount of effort and time individuals spend in seeking information about the availability and activities of others and in providing information to others of their own availability and activities (Herbsleb, Mockus et al. 2001).

Awareness information is multi-faceted. It includes information about people's presence, activities (past, present or future), schedules, routines, deadlines, availability and so on. Moreover, such information may be provided and received through a variety of channels – from physical to social to digital. For instance, by peeking through a partially open office door one may find out whether a colleague is busy. One may also use the knowledge of a colleague's typical routine to infer her availability, or one can consult the colleague's online calendar to check for her availability.

Over the years a variety of (digital) systems have been built with the explicit goal of supporting the collection and dissemination of awareness information. Examples of such systems include Shared Media Spaces (RAVE (Bellotti and Dourish 1997), Portholes (Dourish and Bly 1992), Thunderwire (Hindus, Ackerman et al. 1996)), Shared Calendars, Mailing lists, Shared Workspaces (Polyteam (Mark, Fuchs et al. 1997), BSCW (http://bscw.gmd.de/), Docushare (http://docushare.xerox.com), CVS (http://www.cvshome.org/), Newsgroups), Instant Messaging (e.g. MSN Messenger (http://messenger.msn.com), Yahoo! Messenger (http://messenger.yahoo.com) , ICQ (http://www.icq.com) and AOL Instant Messenger (http://www.aol.com) etc.), Sensors (Active Badges (Want, Hopper et al. 1992), Motion sensors etc.), Shared Displays (Notification Collage (Greenberg and Rounding 2001), Video monitors etc.). Even systems that are generally regarded as single-user such as email and telephone may be employed for awareness purposes. For example, caller ID may be used to screen calls; automatic email replies may be used to indicate extended unavailability and so on.

We find people typically using a combination of diverse systems and mechanisms in their efforts to generate, disseminate and receive awareness information. The manner in which various mechanisms are combined and used depends on the people involved, the task(s), the granularity of the awareness information, the frequency of changes in awareness information, the resources, the cultural norms, the context and so on.

Awareness information assumes a much more important role in the context of the work-related activities of close collaborators – even more so if they are geographically distant (Herbsleb, Mockus et al. 2000). Since we are interested in supporting collaborative work of globally distributed teams, we will focus on studying awareness systems and mechanisms encountered in this scenario.

2. Privacy

Privacy is currently one of the most highly publicized and hotly debated topics. Yet, due to the complexities involved, there exists no commonly agreed upon, precise definition of privacy. The difficulty of precisely defining what privacy is probably stems from the fact that privacy is a highly *situated*, context-dependent concept. Not only that, but even in the *same* situation, different individuals involved may have different opinions and expectations of what privacy means. This fuzziness, context dependency and individual variability makes dealing with privacy a rather difficult task.

Bellotti (Bellotti 1996) points out that two types of privacy definitions are common, to which she refers as *normative* and *operational*. Normatively, Warren (Warren and Brandeis 1890) defines privacy as "freedom to be left alone". Stone et. al. (Stone, Gardner et al. 1983) offer an operational definition of privacy as "ability of the individual to personally control information about oneself" whereas Samarajiva (Samarajiva 1997) extends the definition to "the control of outflow of information that may be of strategic or aesthetic value to the person and control of inflow of information including initiation of contact".

In the physical domain, a variety of mechanisms and artifacts seem to have evolved over time to make privacy management easier. These embody certain social protocols based on some shared assumptions. For example, locking the door to prevent access to others, or knocking on a door before entering even when the door is partially open etc. However, when the shared assumptions behind the embodied social protocols are no longer applicable, for whatever reason – individual, cultural, contextual, task-specific – privacy management once again becomes problematic and privacy violations occur.

Given the inherent complexities involved in privacy management, it is possible that people always harbor some concern regarding potential violation of privacy. The consequences and risks involved may determine the amount of (explicit) effort and time devoted to managing privacy. When the consequences are potentially severe, people may devote considerable attention to preserving privacy. If, despite their efforts, a violation of privacy does occur, individuals typically *negotiate* until a commonly agreed upon state of privacy is reached for everyone involved.

3. Relationship between awareness and privacy

The above discussion regarding awareness and privacy makes the inherent interrelation between the two apparent. The general perception is that there is an inverse relationship between privacy and awareness: more awareness leads to less privacy and vice versa. Even though this may typically be the case, the reverse may also be true, i.e. providing more awareness provides more privacy. For example, maintaining a personal web page allows faculty members to limit the intrusion by requests for copies of their publications (Palen and Dourish 2003). Given the highly situated and context dependent nature of both awareness and privacy, it should be no surprise that the precise manner in which awareness and privacy are dependent on each other is also context dependent. However, regardless of the exact relationship between the two, it is certainly true that they influence each other greatly.

The question, then, is how do people manage the relationship between awareness and privacy – both in the physical domain and in the digital domain. Answering this question involves addressing various sub-questions. Some of these include:

What are the possible benefits to be derived from awareness?
What are the possible benefits to be derived from privacy?
What are people's expectations regarding privacy?
What mechanisms do people use to manage privacy according to these expectations?
How do people deal with violations of privacy?
How do people seek awareness of others?
How do people provide awareness about themselves to others?
How do people deal with conflicts between awareness and privacy?
How do the various domains (physical, social, digital) differ in terms of the affordances they offer for management of awareness and privacy?

4. Privacy in current awareness systems

The current focus in awareness research lies mainly on the awareness of presence or physical activity of others (e.g. talking on the phone, reading email, etc.). In contrast to this, our primary focus is on the awareness of task-related activities, particularly in the context of distributed software development (e.g. progress on a program module, completion of documentation, reporting of a bug etc.). Nonetheless, both foci have underlying similarities that make it instructive for us to study the privacy mechanisms in current awareness systems.

Designers and builders of collaborative awareness systems frequently tend to treat privacy either as a secondary consideration or as an issue for future exploration. This may be due to the underlying assumption that individuals who collaborate with each other have less stringent privacy expectations. The result is often systems with privacy mechanisms that are either too tight or too loose, and have minimal flexibility for modification.

Current awareness systems provide for privacy management through a combination of a large number of mechanisms. The essence of these mechanisms seems to revolve around controlling access (to oneself and one's artifacts) through proper authorization. Different mechanisms differ in terms of who has control, who is authorized and how the process of authorization works. Some examples of privacy mechanisms include access control (e.g., password-protected login), permissions (e.g. UNIX file permissions), assignment of groups and roles, summary and distortion (e.g. abstracting a document, blurring of a video stream (Boyle, Edwards et al. 2000)). These mechanisms may be enacted and enforced in a variety of ways including provision of defaults, generation of *feedback*, enforcing of *reciprocity*, policies and procedures, social consensus and so on.

In reality, control and authorization considerations change dynamically with context. Incorporating this context dependence into the capabilities provided by present systems is problematic, to say the least. Our goal is to study the adequacy of these mechanisms for privacy management and the manners in which they are utilized in current awareness systems. If we know what works (and to what extent) and what does not work, we can look into the *why*, and then use the findings to inform the design of privacy management mechanisms in a general awareness framework.

5. Comparisons of popular Instant Messengers

One of the most popular and widespread contemporary awareness mechanisms is Instant Messaging (IM). IM allows people to indicate their presence to others who are on their "buddy lists". At the same time, it allows checking for the presence of "buddies". It is possible to provide finer-grained information than merely online/offline, by indicating one's current status through various

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase®
Smarter legal research.