Privacy Enhancements for Mobile and Social Uses of Consumer Electronics

Falchuk, B.; Loeb, S.;
Communications Magazine, IEEE
Volume: 48, Issue: 6
Digital Object Identifier: 10.1109/MCOM.2010.5473
Page(s): 102 - 108
Buddy-mapping applications, now possible and deployed on smart phones and personal navigation systems. These kinds of applications can be incredibly useful and fun; at the same time, their feature creep can threaten user privacy.

This article presents middleware architecture and methodology that can help give users of buddy-mapping services greater awareness of who is about to see them before they are actually seen.
INTRODUCTION

Connected mobile consumer electronic devices allow users to take their applications with them wherever they go and weave them into their everyday lives.

Privacy experts believe that a privacy tipping point is one major breach away. But even without a security breach, people are generally apprehensive about the privacy implications associated with location tracking. Recent research indicates that privacy preferences tend to be complex and depends on a variety of contextual attributes.

In this article we take the approach of providing the user with advanced warning of being seen, hence giving the user an opportunity to opt in to this potential privacy threat in real-time.
THE CONTEXT

Figure 1. Typical architecture of a mobile buddy-mapping system.
The about-to-be-seen-related problems rife in today’s buddy-mapping systems are as follows:

• It is currently difficult to manage customized visibility settings when the buddy list is long; the likelihood of forgetting to make a setting for a given user is high.

• No advance warning is given when a user is about to be seen on a buddy’s map.

• Going *invisible or off the grid is a solution*, but is a poor one as it negates almost all of the social benefits of the application.
BUDDY-MAPPING WITH ADVANCED AWARENESS

Figure 2. Architecture of the system at a high level (dashed components are not a part of our own infrastructure).
Within our system, we model and manage encounter horizons (EHs) for all users; an EH is an annotated demarcation at some distance around or near a user’s current location. Logically, each user has an associated series of EHs, each of whose metadata describes the conditions and actions that must occur for about-to-be seen warnings to be generated.
As A is moving towards B; given A's current view on the application map, B is "about to be seen" by A.

Figure 3. Encounter horizons - the dashed EH corresponds to A's map-view range while the others serve as policy triggering thresholds (e.g., for advanced warnings).
Without our system and its capabilities, mobile users are more and more vulnerable to being exposed in situations in which they do not want to be, or, at least, did not plan on. While today’s mobile users are sharing more and more information through blogs, Twitter, and other mobile social networking.
1. User A goes to a job interview at "Company Inc.", a competitor.

3. A's colleague B is nearby, unbeknownst to A. B sees A on his buddy radar map and infers A's motivations.

2. User A forgets to micro-manage his "visibility" and does not have the encounter horizons system.

4. User A never got a chance to recover from his oversight.

Each buddy is near enough to the other to be painted on the others' map.

1. Users A and B both "power up" near each other.
2. Initial context makes them co-visible and the system must use a default or provide the warnings.

Figure 5. Real world scenario (top) and one of several challenging scenarios (bottom).
CHALLENGES AND CONCERNS RELATED TO CONSUMER NETWORKING APPLICATIONS

On one hand, many are enthusiastic about providing peers the ability to peek into their lives, via sharing pictures and ideas with their buddies and via revealing their location in return for social benefits such as unexpectedly bumping into friends.

On the other hand, many have concerns about their privacy and are reluctant to reveal personal information as they cannot anticipate how it will be used.
Figure 6. Example of mobile applications and services of various degrees of mobility and different levels of user privacy control.
CONCLUSIONS

• In this article we present additional middleware-level functionality needed to provide users with the control they may want and need to protect their privacy with respect to how the service operates and in the way it exposes personal information.