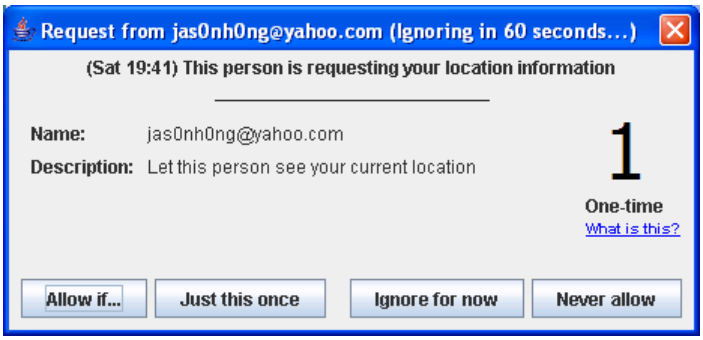
User Interfaces for Privacy-Sensitive Ubiquitous Computing

Jason I. Hong, James A. Landay
Group for User Interface Research, University of California at Berkeley

Over the past decade, there have been significant advances in wireless networks, sensors, and devices of all form factors. These technologies are enabling us to create new kinds of ubiquitous computing applications that can gather and communicate information at unprecedented levels, all in real-time. The problem, however, is that these same technologies also create new privacy risks.

To address this problem, we have developed Confab, a toolkit for building privacy-sensitive ubicomp applications. Confab provides privacy support at three different layers: the *physical layer*, which is responsible for how personal information (such as one's location) is captured; the *infrastructure layer*, which is responsible for how personal information is stored and processed; and the *presentation layer*, which is responsible for user interfaces that give end-users control over and feedback about what personal information is being disclosed to others. Here, we describe our ongoing work at the presentation layer with respect to one's current location.

Confab currently provides some UIs for helping end-users manage their privacy at two different times: *during* a request for personal information (e.g. requesting someone's current location), and *after* a request (e.g., access logs to see who has made requests). The figure below shows an example of the during case, where one individual is requesting another's current location. The large "1" on the right side indicates it is a one-time disclosure (rather than a continuous disclosure), and the options on the bottom provide simple controls over what is disclosed. The "Allow If" case provides more options based on time, for example "Only allow between 9AM and 5PM". If allowed access, the requestor sees the requestee's current place, for example "at home". If denied, the requestor sees "unknown", which is the default.



So far, we have gone through four iterations of this user interface and have evaluated it with nine people in the context of a location-enhanced instant messenger. While the results have been positive so far, there are still many open research questions. Some of these include:

- It is not uncommon for people to lie on the phone when asked what they are doing. Should there be support for "white lies" with respect to location, and if so, how?
- What kinds of tradeoffs are there between simplicity and flexibility? Currently, this UI supports access based on the identity of the requestor and on time. However, some users have also requested the ability to allow access based on physical location.
- Can machine learning be applied to help with decisions? One problem with this UI is that it requires the user's attention to make a decision about disclosure. One could imagine situations where this is not possible, e.g., while driving or while in a meeting. One could imagine using machine learning to help make decisions. For example, "You allowed your spouse access 20 out of the last 20 times. Since you are busy, the system will allow your spouse's current request and inform you of this disclosure."