

Locaccino: A Privacy-Centric Location Sharing Application

Eran Toch, Justin Cranshaw, Paul Hanks Drielsma, Jay Springfield,
Patrick Gage Kelley, Lorrie Cranor, Jason Hong, Norman Sadeh*
Carnegie Mellon University
Pittsburgh, PA

{eran, jcransh, paulhd, jspringf, pkelley, lorrie, jasonh, sadeh}@cs.cmu.edu

ABSTRACT

Locaccino is a location sharing application designed to empower users to effectively control their privacy. It has been piloted by close to 2000 users and has been used by researchers as an experimental platform for conducting research on location-based social networks. Featured technologies include expressive privacy rule creation, detailed feedback mechanisms that help users understand their privacy, algorithms for analyzing privacy preferences, and clients for mobile computers and smartphone devices. In addition, variations of Locaccino are also being piloted as part of research on user-controllable policy learning, learning usable privacy personas and reconciling expressiveness and user burden. The purpose of this demo is to introduce participants to the features of Locaccino, so that they can try out the Locaccino smartphone and laptop applications on their own devices, locate their friends and colleagues, and set rich privacy policies for sharing their location.

Author Keywords

location sharing technology, privacy, mobile social technology

ACM Classification Keywords

H.5.2 Information Interfaces and Presentation: user-centered design; H.5.3 Group and Organization Interfaces evaluation: collaborative computing

General Terms

Human Factors, Design

INTRODUCTION AND BACKGROUND

While location awareness can enhance the user experience in many applications, including social networks and electronic commerce services, it can raise privacy concerns. Empirical evidence shows that users are concerned about who has access to their location [5], and these concerns impact their willingness to use these technologies. Commercial location

sharing applications such as Google Latitude, Foursquare, and Yahoo Fire Eagle, offer coarse and limited control over the conditions under which ones location is shared with others. Common preferences such as “I am only willing to share my location with my colleagues on weekdays between 9am and 5pm and only when I am on company premises” cannot be captured by the privacy settings these applications offer their users.

Locaccino¹ was built to empower users to effectively manage routine every day location sharing privacy preferences. It incorporate findings on the complexity of peoples privacy preferences and the importance of auditing functionality [4, 2, 6] and continues to serve as a basis for experimenting with new user-oriented privacy management functionality. Since its launch in January 2009, Locaccino has been used by close to 2000 users in 67 countries. Locaccino is designed as an open framework, allowing 3rd party applications to securely integrate its location tracking and privacy enforcement capabilities.

Previous studies which empirically investigated people’s privacy preferences in location sharing were mainly based on the short term experience sampling method [1] or on lab studies [3]. Locaccino was designed to incorporate findings of our earlier research in privacy and location sharing, in the context of PeopleFinder [4] (multiple pilots involving several hundred users in 2006 and 2007) and Locution (2008) [6]. Locaccino was designed to be highly scalable and to support large-scale evaluation of different types of user-oriented privacy management functionality.

OVERVIEW OF LOCACCINO

Locaccino leverages the user’s existing social networks on Facebook to facilitate location sharing. Users who connect to Locaccino using their Facebook account are able to request the location of friends who have installed the Locator software. The application comprises two main components:

- **User interface:** The user interface is available both as a web-page and in the form of mobile clients, allowing users to request friends’ locations, set up privacy rules, audit requests for their location, and access other privacy management functionality.
- **Locator software:** The locator software transmits the user’s location to the Locaccino database on a regular basis the

*Primary contact

¹<http://locaccino.org>

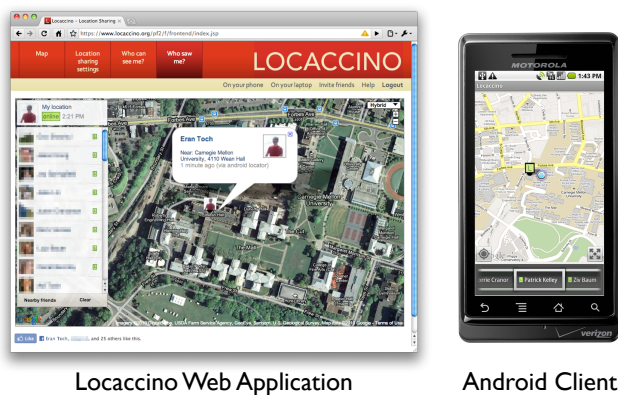


Figure 1. The Locaccino Web application (on the left) and the mobile client installed on an Android phone (on the right). The web application shows the user's friends, and allows the user to configure rich privacy settings. The locator software, installed on smartphones and laptop computers reports the user's location.

frequency of updates varies based on different environmental conditions. Users can install the locator software on their laptop computers (Mac and Windows) or on their smartphones (Android, Symbian and iPhone). The locator determines the user's location using a combination of methods: GPS, cell tower triangulation, and WiFi positioning.

Location Requests

Users can submit requests for the location of their friends. These requests are processed by the Locaccino server in accordance with the privacy settings of the user whose location is being requested. Users also have access to one-click client-based functionality that allows them to override these rules and become "invisible". When a request for someone's location is denied, the response provided by Locaccino is intentionally ambiguous, making it difficult (if not impossible) for the requester to determine whether the target user is currently out of range, has turned off her cell phone, has become invisible or does not have a rule allowing this specific request.

Privacy Controls

Users control their location sharing preferences by managing location disclosure rules. When first adding the application, the default disclosure policy is to deny all requests. Rules are constructed from three criteria that grant access, called "restrictions", all of them should be satisfied by the incoming request:

- **Friends (Who):** Friend restrictions specify individual Facebook friends, groups of Facebook friends, or whole Facebook Networks (e.g. the "Carnegie Mellon" network) with whom a user is willing to share his or her location information.
- **Time (When):** Users can define time spans (i.e. 9 am - 5 pm) and days of the week during which they wish to allow others access to their location information.

- **Locations (Where):** Users can define and manage the geographic areas where they wish to be located.

In addition to allowing for the creation of rich privacy rules, Locaccino allows users to review the complete log of requests made for their location. Users can review who made each request, and whether it was allowed, denied, or if they were offline or hidden. Users can also view a map of where they were at the time of the request. Additionally, Locaccino allows users to view who can currently locate them, which helps users evaluate their rules.

OPEN API

Locaccino provides secure access to 3rd party applications using an Application Programming Interface (API). The API is actively used by Locaccino clients to send and request locations and access some of the privacy controls. Users can control the API access rights to individual applications using the familiar rules interfaces, creating a secure and trustworthy environment for ubiquitous computing research.

ACKNOWLEDGMENT

This work has been supported by NSF Cyber Trust grant CNS-0627513, NSF Trustworthy Computing grant CNS-0905562 and ARO research grant DAAD19-02-1-0389 to Carnegie Mellon University's CyLab. Additional support has been provided by Google, Microsoft through the Carnegie Mellon Center for Computational Thinking, FCT through the CMU / Portugal Information and Communication Technologies Institute, and grants from France Telecom and Nokia.

REFERENCES

1. D. Anthony, D. Kotz, and T. Henderson. Privacy in location-aware computing environments. *IEEE Pervasive Computing*, 6(4):64–72, 2007.
2. M. Benisch, P. G. Kelley, N. Sadeh, and L. F. Cranor. Capturing location privacy preferences: Quantifying accuracy and user burden tradeoffs. Technical Report CMU-ISR-10-105, Carnegie Mellon University, March 2010.
3. S. Consolovo, I. Smith, T. Matthews, A. LaMarca, J. Tabert, and P. Powledge. Location disclosure to social relations: Why, when, & what people want to share. In *CHI '05*, 2005.
4. N. Sadeh, J. Hong, L. Cranor, I. Fette, P. Kelley, M. Prabaker, and J. Rao. Understanding and capturing people's privacy policies in a mobile social networking application. *Personal and Ubiquitous Computing*, 13(16):401 – 412, 2009.
5. J. Tsai, P. Kelley, and L. C. ad Norman Sadeh. Public perceptions of the risks and benefits of location-sharing technologies. In *37th Research Conference on Communication, Information, and Internet Policy (TPRC)*, 2009.
6. J. Tsai, P. Kelley, P. H. Drielsma, L. F. Cranor, J. Hong, and N. Sadeh. Who's viewed you? the impact of feedback in a mobile-location system. In *CHI '09*, pages 2003–2012, 2009.