Sharing Everyday Places I Go While Preserving Privacy

Pamela J. Ludford
University of Minnnesota,
Department of Computer Science
4-192 EE/CS Building
200 Union St. SE
Minneapolis, MN 55455 USA
ludford@cs.umn.edu

CHI 2006, April 22–27, 2006, Montréal, Québec, Canada.
ACM 1-59593-298-4/06/0004.

Abstract
Several new location-based information applications reveal *sets of places* that an individual frequently visits. This practice gives rise to related privacy questions and new interface needs. For example, while electronic system users want to be in control of private data and know how those who have it will employ it [10], there are no design guidelines for garnering informed consent for using place-based information. In addition, the set of places a person frequents may reveal information such as: 1) when they are likely to go to a place, or 2) within close proximity, where they live. If a user considers this information private, they may still inadvertently disclose it: humans have difficulty comprehending aggregate effects of their actions [1]. A system could therefore deliver benefit by identifying notable risks and informing the user. This research plan will address these key issues and will ultimately inform privacy interface design.

Keywords
Location privacy, informed consent, location-based reminder, local search, data visualization, place set.

ACM Classification Keywords
H5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous.

Introduction

Until recently it was difficult to collect a digital history of places that an individual frequently visits. Many new applications gather this information in various forms, including place-based recommenders, location-based friend-finders, place annotation systems such as GeoNotes [3] or PlaceOpedia (www.placeopedia.com), and location-based advertising systems. While people consider their presence at certain places private [2], current systems do little to assist them in deciding which place-based information to disclose. The goal of this research is therefore to uncover design guidelines that provide attractive, fast, and informative interfaces that help users manage privacy concerns in this realm.

We define *place* as one, or a contiguous set of latitude/longitude points: it is often a building or locality; it can be an open space such as a park or corner bus stop. We differentiate a *place* from a *path*, which is a contiguous line of latitude/longitude points: it represents a route between places.

Other researchers have studied preferences for revealing one's real-time presence at a place [7]. Our work differs: rather than current location, we study the set of places a person tends to visit over time. For a head of household this might consist of work, the grocery and hardware stores, child-activity places, etc. In a preliminary study, we found subjects had concerns about revealing locations they commonly frequent, even in anonymous format. These results motivate our research. To guide our efforts, we pose 3 high-level research questions (RQs):

RQ1: What are user's concerns about revealing places they frequently visit, and how can we best study them?

RQ2: How can we successfully inform users about the effects of location-based information disclosures?

RQ3: What personal information can a person's place set reveal about them, and what is their comfort level with others knowing this information?

Our overall goal is to inform interface design: we seek to minimize the effort needed to protect privacy.

Research Application Platforms

We will use 2 location-based systems as research platforms: PlaceMail, a personal location-based reminder system, and a LoGo, a new map-based community local search. First, PlaceMail runs on a cell phone and with it, people leave errand-related messages for themselves at places they frequent [9]. The cell phone uses GPS to sense their location, and messages are delivered when they near a place with an outstanding message. As a by-product of use, PlaceMail users develop a list of everyday places they go.

Second, LoGo offers functionality similar to map-based local search tools like Google Maps[1]: with either tool, a person can (1) view a geographic locale on a map and (2) search for places (such as restaurants) in the locale. LoGo differs, however, because it gets its place data from people who frequent the area. In contrast, Google and others get place data from a commercial vendor such as Navteq. Himmelstein finds the latter's place data incomplete and lacking character [6], so LoGo stands to improve on the commercial systems. For much of our research, PlaceMail users will consider implications of contributing their everday places to LoGo, thus putting it in public view.

---

[1] http://www.maps.google.com

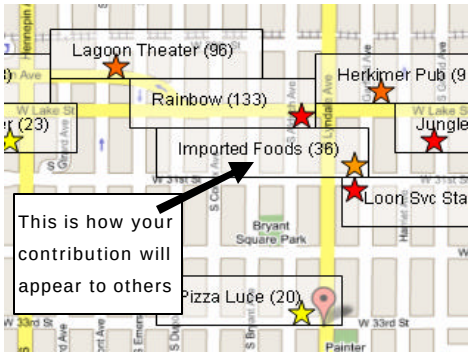

Figure 1. Currently under development, the Visual informed consent interface will show users how their data will appear to the public if they contribute it to LoGo, a map-based local search engine. With this view, users can see contextual information that may influence their contribution decision.

Our main research activities will include 1) designing, evaluating, and reporting on a graphical informed consent interface for contributing data, and 2) studying the information that a person's everyday place set can reveal about them.

Visual informed consent displays

Local search contributors want to understand the effects, both good and bad, of the information they offer [4]. Further, a single contribution (such as adding a place to the search engine) may have multiple effects. We want to depict these multiple effects in a user-friendly format, but have few good interface examples to follow. This is because many systems do not currently tell the user how (or if) they employ collected data [4]. If they do, the explanation generally consists of a lengthy text-based statement that users rarely read [8]. Our goal is to pioneer an interface that people will view and understand.

We are currently building a visual informed consent interface that illustrates how local search will use contributed information, and we will seek to understand how it is received by users. For example, do they consult it? Do they understand the presented information? Does it contain information necessary to make a disclosure decision? The outcomes can influence the consent process in other location-based information systems, as well as other settings where a visual consent display is workable. A prototype appears in Figure 1.

We anticipate evaluating the interface in a lab study where PlaceMail users will employ it to determine whether to contribute places to LoGo. We will compare performance of the graphical interface to a text interface providing similar information.

Identifying and Preventing Sensitive Information Disclosure

Next, contributing location-based information to a community presents a unique set of risks: in aggregate, a person's contributions may reveal unintended details about their location-based habits. For example, how closely can an adversary determine where a person lives, works, or when they are likely to frequent a place based on their place-related contributions to an online community? Since no others have explored this topic, we will examine when a set of location-based information is apt to reveal sensitive personal information, develop algorithms to detect these situations, and identify solutions for preventing contributors from unintentionally disclosing private information.

We also will explore people's sensitivity to revealing location-based proximity. For example, would a data contributor feel safe if a stranger can determine within six blocks (or two blocks, or a mile) where they live? We will examine this issue to learn 'how close is too close' from the contributor's standpoint. This framework can guide location-based information system designers, such as those building place-based recommenders or annotation applications. We will also explore related questions:

How often do people make unintended location-based information disclosures? Although a host of others have studied location privacy issues, none have studied whether those who contribute to location-based information are aware that they might be revealing aspects of their location via the aggregate of their contributions. The results can affect informed consent interface design.

How should an interface mitigate revealing sets location-based contributions? If a person is about to contribute a set of revealing location-based information, should the system automatically conceal their contributions from public view? Or should it alert the user to the risk and let them mitigate the situation? Related research does not directly answer this question: Friedman et al. say if an informed consent process takes too long, potential contributors will default to always saying 'no' to contribution requests [5]. This favors a system that automatically cloaks revealing data. For example, the system could automatically hide data contributions that are strong determinants of where a person lives from public view. On the other hand, users say they want to control their private information [4], which suggests an interface where they directly manage the situation. We will explore these juxtaposed alternatives (as well as hybrids of the two), and deliver guidelines that will guide designers in handling this dilemma.

Acknowledgements

This research is funded by NSF grant IIS-0307459. Many thanks to my advisor Loren Terveen for his constant support of my research, and to Jonathan Grudin for providing valuable insights on this dissertation plan.

References

[1] Acquisti, A. (2004). Privacy in Electronic Commerce and the Economics of Immediate Gratification," Alessandro Acquisti. *In Proc., ACM Electronic Commerce Conference, ACM Press*, 21-29.

[2] Barkhuus, L., Dey, A. (2003). Location-Based Services for Mobile Telephony: a Study of Users' Privacy Concerns. *Proceedings of the IFIP Conference on Human-Computer Interaction, INTERACT, p. 709-712.*

[3] Espinoza, F., Persson, P., Sandin, A., Nyström, H., Cacciatore. E. & Bylund, M. (2001) GeoNotes: Social and Navigational Aspects of Location-Based Information Systems, in *Abowd, Brumitt & Shafer (eds.) Ubiquitous Computing, International Conference*, Berlin: Springer, p. 2-17.

[4] Federal Trade Commission (2000). Privacy Online: Fair Information Practices in the Electronic Marketplace (A Report to Congress). Federal Trade Commission, Washington, D.C., May, 2000.

[5] Friedman, B., Howe, D., (2002). Informed Consent in the Mozilla Browser: Implementing Value-Sensitive Design. Proceedings of the 35th Hawaii Intl. Conference on System Sciences.

[6] Himmelstein, M., (2005). *Local Search: The Internet Is the Yellow Pages*, IEEE Computing,Volume: 38, Issue: 2 p. 26- 34.

[7] Iachello, G., Smith, I., Consolvo, S., Abowd, G., Hughes, J., Howard, J., Potter, F., Scott, J., Sohn, T., Hightower, J., Lamarca, A. (2005) Control, Deception and Communication: Evaluating the Deployment of a Location-Enhanced Messaging Service. *In Proceedings of the Intl. Conference on Ubiquitous Computin, Tokyo, Japan. September 2005*

[8] Jensen, C., Potts, C. (2004). Privacy policies as decision-making tools: an evaluation of online privacy notices. *Proceedings of the SIGCHI conference on Human factors in computing systems, ACM Press*. p. 471-478.

[9] Ludford, P., Frankowski, D., Reily, K., Wilms, K., Terveen, L. (2006). Because I Carry My Cell Phone Anyway: Functional Location-Based Reminder Applications. *To appear in Proc. CHI 2006.* http://www-users.cs.umn.edu/~ludford/placemail_submit.pdf

[10] Taylor, H. (2003). Most People Are "Privacy Pragmatists" Who, While Concerned about Privacy, Will Sometimes Trade It Off for Other Benefits. *The Harris Poll®* #17, March 19, 2003.