

Representing Location in Location-based Social Awareness Systems

Michael Voong

School of Computer Science
Birmingham, UK B15 2TT
+44 (0) 121 414 2790

m.voong@cs.bham.ac.uk

Russell Beale

School of Computer Science
Birmingham, UK B15 2TT
+44 (0) 121 414 3729

r.beale@cs.bham.ac.uk

ABSTRACT

We analyze the results of a survey distributed to heavy users of social networking website on current mobile communications practices regarding location disclosure. We discovered that deception on location disclosure is a common practice amongst this demographic. We also discovered privacy issues of location are reduced in line with cue accuracy.

We discuss the social behavior of deception in location sharing, and discover that online social network users are more open to revealing location, but more likely to be deceptive. We demonstrate the user interface of a mobile location-based awareness system that allows the user's location cue and disclosure accuracy to be set explicitly.

Categories and Subject Descriptors

H.1.2 [User/Machine Systems]: Human factors, H.5.m [Information Interfaces and Presentation (e.g., HCI)]: Miscellaneous

General Terms

Design, Human Factors

Keywords

Social awareness, location, deception, mobile, connectedness, design guidelines

1. INTRODUCTION

Modern communications technologies facilitate serendipitous interaction between peers, fitting naturally into the fabric of everyday life. This technology supports micro-coordination, a term used to describe the constant flow of communication between people, keeping them up-to-date on happenings [1]. Different modes of communication afford different social practices; various mediums carry different affordances that develop in society over repeated use. Paper mail has not been completely replaced by email, nor has the telephone replaced letters.

New social communications websites such as Facebook and

Twitter show the thirst of millions to stay hyper-connected to members of their social networks. One of the first commercialized location-based systems was launched in 2002 by KDDI in Japan, a ubiquitous location-based person finder. More recently we have seen a wider adoption of commercialized friend-finding applications such as Helio's Mobile Buddy Beacon, Boost Mobile's Loopt and GyPSii. Controlling location disclosure is a salient issue in these systems as they reach out to more than just close friends; people become more self-conscious of how their location is perceived by the systems and others.

When location is used as a context-indicator to facilitate location-based search, there are little privacy issues as the data only flows between the service provider and the user. However, when locations are shared to others, the issue is more complex [2], raising issues of privacy, plausible deniability, uncertainty, self-perception and notions of place vs. activity [3, 4]. Indicating exact locations result in the surfacing of major privacy problems. Changing the representation to display a less accurate location cue has been shown to reduce this problem, but may result in users feeling less in control [3].

The literature has shown that denial (rejection), deception (false locations) and evasion (busy/away) are important social practices that need to be carried into these systems [3]. The authors write: "understanding these denial and restraint strategies, and supporting them explicitly in new technologies, will be an essential condition for the acceptance and, ultimately, the success of pervasive technologies". In the pilot study described, however, users were found to rarely deceive others. This observation can be attributed to many things, including timing, the high level of trust in the self-selected study group. Recreational times of the year, for example, could have affected the results, as would selective sharing to trusted friends. There is much literature in psychology on the nature of lying, and it was found that there are significantly different reasons for lying, classified into "self-centered", "other-oriented" and "altruistic", depending on whether the other person is a stranger, close friend or romantic partner [5].

We are trying to find ways to visualize personal location cues that reduces privacy concerns by considering current social behavior of location sharing into designs. Schmandt and Marmasse discuss a system that encodes location data into a less interpretable user-defined label, e.g. "in the city" or "out" [6]. Other research has shown that using mappings of location data into a categorical representation of *moving* or *not moving* can often be enough to alleviate many of the privacy issues at play [7, 8]. Although these flexible labels must be manually kept up-to-date, they offer a level of expressiveness that a pinpoint location indicated on a map cannot. In addition, the

© The Author 2008.

Published by the British Computer Society

requirement for adjustments to be explicitly made by the user keeps the user *in control*.

With the proliferation of online social networking, people often add hundreds or even thousands of ‘friends’, many of which are even strangers or mere acquaintances. We constructed a study to capture the relationship between social networking usage and the privacy issues of location sharing, and to capture the existing behavior of location sharing with the goal of improving location-based social awareness systems.

2. STUDY

A survey was distributed primarily to students present on a University network on Facebook (N=144). That particular demographic tends to use Facebook for social connection, social investigation, social network surfing and status updating [9]. We wanted to answer the broad question of “how should we design a mobile location-aware application targeted at people active on social networking websites, based on current behavior of location disclosure”.

In total, 126 users completed every question that was set. The largest age group was 16-29 (87.3%), with the main category being 20-24 (57.9%). 57.1% of respondents were in undergraduate higher education and 38.9% in or have finished postgraduate education. The four main ethnic origins were Chinese (35.7%), White – British (32.5%), White (9.5%) and Asian or Asian British-Indian (7.1%), making up a total of 84.8% of the respondents.

One focus of our analysis was to obtain information about in what situations users are willing to share their location, what factors affect people’s decisions to be deceptive, and how this relates to patterns of social network use.

2.1 Main Findings

We found that a significant proportion of respondents expressed a regular use of deception when sharing locations over existing communications technologies. We also found the correlation between the importance of social networking websites to a user and a) self-reported, perceived frequency of deception to be *negative* and b) openness to sharing to be *positive*. One possible interpretation is that while users justify, and are content with revealing location (even more so when the use social networking sites more), they still want control over what location they want to reveal - including false ones. These results will be discussed in more detail later.

2.2 Current Communication Technologies

The results showed that our demographic held a great reliance on communications technologies to keep in touch with friends and family, which was expected from heavy Facebook users. The survey asked respondents to specify on a 7-point Likert scale (Extremely Important – Extremely Unimportant) for 7 different approaches to electronic communication (instant messenger, email, voice calls, video + voice calls, SMS, websites, other online). We found that IM (82.4% important), email (93%), voice (92.3%) and SMS (93%) were viewed consistently strongly as being important for friends and family communication. As a comparison, voice + video technologies such as Skype were important for 28.9%, websites (48.6%) and other (18.3%).

2.3 Factors Affecting Disclosure

Measured on a Likert scale from 3: extremely important to -1: extremely unimportant, the three most important factors affecting whether the location of the user would be disclosed, in decreasing order of average importance were requester identity, relationship with requester and reasons for asking. The means

are shown in Figure 1. The highest rated factor, requester identity, was in line with an ESM-based study conducted by [10].

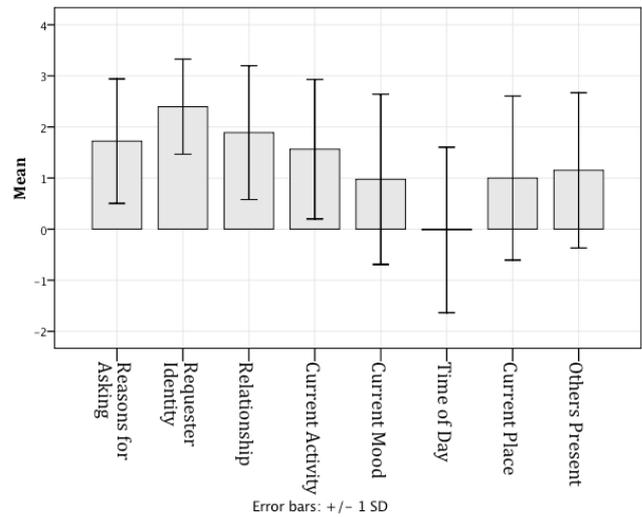


Figure 1. Importance of reasons for disclosure

2.4 Location Deception

The issue of the privacy of location disclosure has been often discussed in the literature. For example, [10] focused on whether people want to disclose location or not, dividing groups into pragmatists (“what’s in it for me?”), fundamentalists (skeptics) and unconcerned (privacy a non-issue). This issue is more complex; not only do we consider when people wish to withhold their location; we need to consider when they want to lie about it. Our results (see Figure 2) show the self-reported frequency of deceptive practice when asked about their location (N=126).

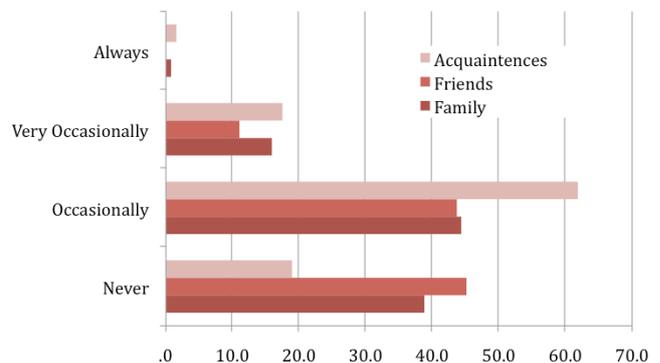


Figure 2. Location disclosure self-reported lying frequency (percentage)

Deception towards acquaintances happens most often, at 61.9% (occasionally) and 19.0% (very occasionally). This is understandable, given that people tend to be wary of the information we give away to people we do not feel should know the information. Family and friends show similar results. The significant result here is that only 38.9%, 45.2% and 19.0% specified themselves as never lying to family, friends and acquaintances respectively.

2.5 Reasons for Location Deceptive Practices

Respondents were asked to write about why they sometimes disclose deceptive locations.

One reason was *appropriateness of place* (“somewhere I shouldn’t be”). Users mentioned examples such as to “save embarrassment or to protect another lie!”, “unsuitability of venue (to family for instance)” or “to hide my real location – perhaps embarrassing”.

An *engineered situation* where lying is beneficial to keep the plan into place was also given, e.g., a secret party: “with family/close friends - when organizing a surprise party/event and do not want to disclose location”.

Current context and feeling (not wanting to be disturbed/avoid people) was another major reason. Respondents commented: “At the time I may not feel like seeing said person or having them know where I am”, “not wanting to be disturbed, or perhaps I know my parents wouldn’t agree with me being somewhere (i.e. the pub, etc) when they know I have work to do, so I’d just not say :)”.

Reasons for requesting was another factor: “if don’t need to know, won’t tell them (nosy)”, “sometimes I do because I don’t like how nosy someone is being”, “fear of stalker”. This is when and understanding of the reasons that the person is requesting such data is required. This was also discovered in another study [10], and if a reason is not found, people may prefer to give a false answer.

Users said that they often lie for reasons of protecting their own image of *punctuality*: “being late”, “being somewhere not suppose to be”, “I could be running slightly late for a rendezvous.” These lies rarely have large consequences – and are more often used as a means of creating psychological comfort.

Another category was *social exclusivity*: “I want to be alone or with some other friends”, “Not to hurt someone’s feelings, to avoid someone annoying”. At times the person may be reluctant to give away information because they are in an exclusive social situation that may be desirable for the requester to also take part in.

The current *relationship with the requester* was an important deciding issue: “...sometimes there are people you just don’t want to be at that party!” Humans are complex social beings, and relationships constantly change.

People may want to *fake an activity*. An example action, given by a respondent, is “pretending to be busy”. This highlights the importance of implementing mechanisms to allow activities to be faked, which is difficult when locations are being automatically disclosed. This behavior can be seen in typical IM use; people appear to be busy through their indicated status, but in reality this may be to block less-important messages, for other reasons.

2.6 Online Privacy vs. Location Privacy

We form the hypothesis that people that are more reliant on social networking websites for family/friend communication are statistically more likely to not mind revealing location, and reliance is positively correlated to deceptive behavior. Social networking websites requires a high level of social information disclosure for maximum gain, and one could reasonably predict that heavy users would tend to have less problems with disclosing location.

The survey formed scenarios including the following: at a night club/bar, on holiday, at my favorite café, in the city centre. For each of these scenarios, respondents were asked to select yes/no on whether they would share their location to a) family, b) close friends, c) acquaintances and d) strangers, given a system that enables automatic location disclosure. The mean response was taken as a metric of how open the respondent is when it comes

to location disclosure. A metric for social network importance was taken from responses of important they felt the sites were for keeping in touch with friends and family.

Mean social network importance vs. openness to sharing was positively correlated ($r_s=0.180$, one-tailed, $N=126$). However, mean social network importance vs. perceived deception frequency was significantly *negatively* correlated ($r_s=-0.170$, one-tailed, $N=126$ at 0.05 level). This shows a corresponding increase in deception frequency as issues with personal information privacy reduced. We argue that a model that assumes personal privacy as being the primary factor in controlling location disclosure is over-simplistic; it must also take into account deception practices, in-line with previous studies [3, 8].

2.7 Location Representation

In many situations, humans have the tendency to respond to requests for details ambiguously. For example, if we were asked of our location most of the time we would reply as vaguely as possible, considering variables such as our interpretation of what the information seeker wants, our current context, and ability to meet up due to distance [10]. The best way to visualize location information may not be through undistorted map-based representations where spatial browsing can be clunky – but a more dynamic view that is based around positions relative to landmarks/places. This may also be more in line with the way people are thought to remember spaces and navigate them (see theories of cognitive maps [13]).

Privacy concerns were found to depend on the level of detail of the location visualization. We asked respondents to provide on a Likert scale of 1–7 (strongly concerned – strongly unconcerned) their privacy concerns in situations when their *absolute pinpoint* location is made visible (to a controlled list of people), compared to relative, landmark-based, *less detailed* visualizations (means = 5.39, 4.80 respectively, s.ds = 1.65, 1.68).

One respondent said: “A good idea would be a map that shows your friends location in relative geographical terms. If you enter the city centre the map would give a rough picture of their location. This could be say, friend A is situated in the Bullring or Friend B is at New Street station. A map giving the exact location of each friend is a little creepy in my opinion”.

2.8 APPLIED SYSTEM

When people are asked “where are you?”, they answer based on a variety of reasons. Although our study may not have captured every reason, we can draw reasonable conclusions of general deceptive behavior. The study confirmed that people do deceive, and the reasons are given in the quotes.

Most existing commercial friend tracking systems locate users as accurately as possible and share this information to others. Our results on the reasons why people choose to disclose or not show that the identity of the requester is still the most important factor. This is true for approaches where individual requests are sent when information is to be disclosed [3], but when the aim is to perpetually disclose location, we need to carefully consider how to carefully control cue representation [11, 12], to reduce the privacy problems of sharing the information to some acquaintances as well as close friends and family.

We applied the results of our study to the design of a mobile social awareness system that uses GPS to send locations to a server (Figure 3). Users define place labels in advance on a searchable map to indicate landmarks of importance such as “Selly Park”, “night life” or “city centre” and carry the J2ME application on their mobile phone. A list-based representation

was chosen over a map-based representation, as it would otherwise be difficult to indicate blurred locations clearly on a small map on a mobile screen. Other users are shown under their current places, as indicated by the labels.

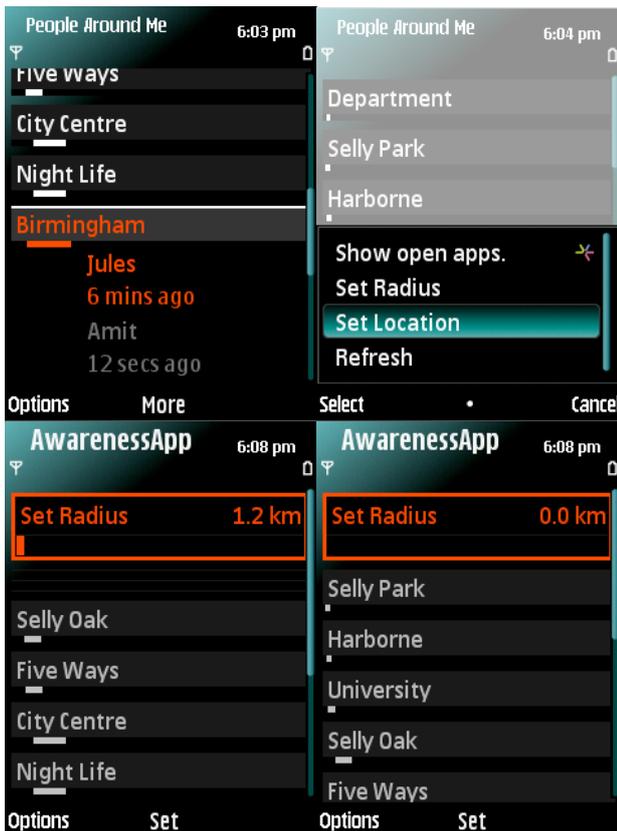


Figure 3. Working implementation shown on a Nokia J2ME emulator based on deception behavior and privacy results

All: **ambiguity of representation**: users may be in the city centre of Birmingham, but wish to be represented in the broader label of Birmingham. The bars represent relative distances from the user's reference point and geographic width of the places, which helps users visualize distances between places.

Top-right: **location modification**: the location can be moved relative to landmarks that are set by users in advanced.

Bottom row: **modification of the disclosure circle's radius** to change the accuracy of location disclosed; the list updates to reflect the possible interpretations. By setting a smaller radius, other users can see a more accurate location. A combination of explicitly setting a user's location and changing the accuracy of disclosure with the concept of a disclosure radius protects the privacy of individuals when they need it, and allows them to carry out their usual location disclosure behavior.

3. CONCLUSIONS

We have discussed how the representations of location in existing systems need work to agree with social behavior of deception sharing. We found that deception is a casual but apparent process and argued that this must be accounted for in social awareness interfaces. In the light of these results we lay out design suggestions, demonstrating a working mobile user interface that allows the modification and 'fudging' of user's locations.

4. FUTURE WORK

Using this platform, we are studying how we can combine location cues with ones formed from carried accelerometers, and how to form valid effect measures of connectedness between users.

5. REFERENCES

- [1] Grinter, R.E., Palen, L. and Eldridge, M. 2006. Chatting with Teenagers: Considering the Place of Chat Technologies in Teen Life. *ACM Transactions on Computer-Human Interaction*, 13, 4, 423–447
- [2] Barkhuus, L. and Dey, A. 2003. Location-Based Services for Mobile Telephony: A Study of Users' Privacy Concerns. In *Proceedings of Interact*, 709–712.
- [3] Iachello, G., Smith, I., Consolvo, S., Abowd, G.D., Hughes, J., Howard, J., Potter, F., Scott, J., Sohn, T., Hightower, J. and LaMarca, A. 2005. Control, Deception, and Communication: Evaluating the Deployment of a Location-enhanced Messaging Service. In *Proceedings of UbiComp '05: Ubiquitous Computing*, 213–231.
- [4] Girardin, F. 2007. Bridging the Social-technical Gap in Location-aware Computing. In *Proceedings of CHI '07: Extended Abstracts on Human Factors in Computing Systems (New York, NY, USA) ACM Press*, 1653–1656.
- [5] Ennis, E., Vrij, A. and Chance, C. 2008. Individual Differences and Lying in Everyday Life. *Journal of Social and Personal Relationships*, 25, 1, 105–118
- [6] Schmandt, C. and Marmasse, N. 2004. User-Centered Location Awareness. *Computer*, 37, 10, 110–111
- [7] Bentley, F.R. and Metcalf, C.J. 2007. Sharing Motion Information with Close Family and Friends. In *Proceedings of CHI '07: The SIGCHI Conference on Human Factors in Computing Systems (New York, NY, USA) ACM Press*, 1361–1370.
- [8] Smith, I., Consolvo, S., Lamarca, A., Hightower, J., Scott, J., Sohn, T., Hughes, J., Iachello, G. and Abowd, G.D. 2005. Social Disclosure of Place: From Location Technology to Communication Practices. In *Proceedings of Pervasive Computing (Berlin / Heidelberg) Springer*, 134–151.
- [9] Joinson, A.N. 2008. Looking At, Looking Up Or Keeping Up with People?: Motives and Use of Facebook. In *Proceedings of CHI '08: The SIGCHI Conference on Human Factors in Computing Systems (New York, NY, USA) ACM*, 1027–1036.
- [10] Consolvo, S., Smith, I.E., Matthews, T., LaMarca, A., Tabert, J. and Powledge, P. 2005. Location Disclosure to Social relations: Why, When, & What People Want to Share. In *Proceedings of CHI '05: The SIGCHI Conference on Human Factors in Computing Systems (New York, NY, USA) ACM Press*, 81–90.
- [11] Bellotti, V. and Edwards, K. 2001. Intelligibility and Accountability: Human Considerations in Context-aware Systems. *Human-Computer Interaction*, 16, 2, 3 & 4, 193–212
- [12] Gaver, B. 2002. Provocative Awareness. *Computer Supported Cooperative Work (CSCW)*, 11, 3, 475–493
- [13] Tversky, B. 1993. Cognitive Maps, Cognitive Collages, and Spatial Mental Models. In *Proceedings of Spatial Information Theory: A Theoretical Basis for GIS: European Conference Springer*.