# Locate! – When do Users Disclose Location?

Maija Poikela[a] Robert Schmidt[b] Ina Wechsung[a] Sebastian Möller[a]

Quality and Usability Lab, Telekom Innovation Laboratories, TU Berlin

[a] firstname.lastname@telekom.de, [b] mail@robschmidt.de

## ABSTRACT

Location information and traces (via tracking) can reveal vast amounts of information about a user: where she lives, works, and even which restaurants or friends she visits. Therefore, this information should be handled with sufficient concern and care. Willingness to disclose one's location is influenced by various factors including who is asking the location and what the reason for the location request is, as well as individual characteristics such as one's privacy concerns.

This paper outlines a study aimed at determining the relationship between these factors and users' willingness to share their location with others using a mobile device. To study this, we developed a mobile application that lets the users share their current location with others at various levels of accuracy. Using the application, we ran a field study simulating the communication between the participants and their various contacts. Our results show that mainly the personal, rather than external factors influence the tendency for location disclosure. Users with lower privacy concerns regarding the accuracy of personal information share their location with more accuracy. Also, people who generally feel close with others tend to disclose their location more accurately.

## 1. INTRODUCTION

Location-based systems have become increasingly widespread sharing users' location information to a variety of application providers. Due to this information now being readily available, privacy concerns can be quite well-grounded when using location-based services. A complete user profile can be built based on not only the user's online presence and active self-disclosure, but also based on one's location information. The user needs to be aware of the implications of revealing one's location in order to take the required precautions towards limiting the information that is revealed to others.

Despite there being justified discussion on privacy intrusiveness around the location-based applications, they are widely accepted. Earlier studies suggest that even if the users have high privacy concerns, their disclosing behavior might not be in line with these concerns [1]–[4]. Users might state being fundamentalists when it comes to privacy-related issues, but still in some situations disclose all their personal information. This phenomenon is explained by earlier studies suggesting that people are willing to give up their privacy to a certain extent if the service they receive as an exchange is found useful [5]. This added benefit can be for example getting helpful information, or facilitated social interaction.

Interpersonal matters play an important role when users interact with others using technology on an everyday basis [6]. When users try to assess whether to disclose information, they need to understand, or guess, how the information that they share would be interpreted by others. Thus, for social reasons, users might feel pressured to disclose more than what they would otherwise feel comfortable with. According to the social penetration theory [7], the interpersonal disclosure has different intimacy layers, and more intimate disclosures happen in close relationships where these layers have gradually been penetrated.

### 1.1 Related Work

According to previous studies, the users' willingness to share a location depends on who is requesting it, why the requester wants to know the location information, and what level of detail is most relevant for the requester [8], [9]. Amongst these factors, who asked for location information seemed to be a bigger influencing factor than context [10], [11]. This seemed to hold true also in an earlier online survey where the users stated having concerns about sharing their location information online, and in particular, being extremely concerned about who has access to their location information [12]. Based on an earlier study by Consolvo et al. [8], the degree of precision of the disclosure of privacy information seems not to be the key parameter in the disclosure. According to the study, the users rather tend to share their location at an accuracy that they find most relevant for the requester.

According to the study by Iachello et al. [13], the users would in certain situations ignore messages or not carry their mobile phones with them with the intention of being unavailable to others. In the same study, the users seemed to prefer responding to a location request with an activity rather than a location. Apart from the context and interpersonal variables, personal characteristics also seem to dictate the users' willingness to share [9]. It seems that the privacy and disclosing preferences are affected by various factors and are complex, as also stated earlier by Sadeh et al. [14].

### 1.2 Our Study

Based on these findings, we wanted to study how users' privacy concerns, and other variables such as context, who the requester is, and interpersonal closeness with this person, affect their location sharing behaviour. As users' disclosing intentions might not be in line with their actual behaviour [3], we wanted to study this in an experiment that would be as realistic as possible, and also give the users a chance to choose how accurately they wanted to disclose, if at all.

We developed a mobile application called "Locate!" that lets users share their location at various different accuracy levels, as well as deny or fake their location if they chose to. The users could also share some contextual information in addition to the location. For this, we provided a drop-down menu with pre-

Symposium on Usable Privacy and Security (SOUPS) 2014, July 9-11, 2014, Menlo Park, CA.

selected items for semantic location. Additionally, the users could type in an additional message using the provided comment field.

We ran a seven-day field study using this app, wherein the users responded on location requests from various contacts (requesters) from their address book.

# 2. RESEARCH METHODS

## 2.1 Design of the Mobile Application

Locate! is a prototype where the users can respond to location requests. The application has the look and feel of a normal messaging application, the biggest difference being that the user cannot request a location of another user. Apart from this, the interaction is made as realistic as possible to overcome the issues of studies of disclosure in hypothetical settings. The requests are sent to the users simulating actual messages, using a set of contacts from their address books.

### *2.1.1 Determining the Accuracy of Shared Location*

We expect that the users would, based on each situation, prefer to fine-tune the accuracy of shared location rather than being able to choose simply between sharing or not sharing. To accomplish this, we gave the users an option to choose how accurately they wanted to share their location.

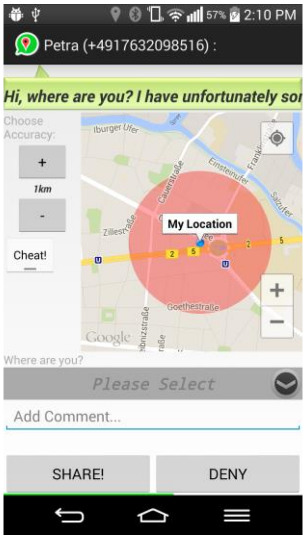
*Blurring* has been proposed as a technique to add privacy by increasing ambiguity [15]. The advantage of such approach is that this provides an alternative to simply disclose or not. Blurring can be implemented for example by not providing the most accurate location. In some cases, a more vaguely shared location might be adequate, and exact disclosure would unnecessarily intrude the users' privacy.

The user could change the accuracy between 25m and 100km, and the default accuracy was randomized. The location accuracies were chosen to correspond to semantically meaningful accuracies for the user, such as the exact location (25m), a block (100m), or neighbourhood (500m). The accuracy of sharing could be chosen using the controls on the side of the user interface. For visualization, the user sees a map with a circle around the location she is about to share, and the visualization area would adapt to the changes in chosen location accuracy accordingly (Figure 1).

Earlier studies have suggested that, as a means to protect one's privacy, users would rather ignore requests than be deceitful [13], However, in some situations ignoring would not be appropriate, but it might also be socially awkward to share one's actual location, or to deny sharing. We expect that in such situations it would be more appropriate to be deceitful rather than force honesty, even if with blurring. To enable also non-trutful disclosure, the user could also share a faked location with an accuracy of one's choice (Figure 2).

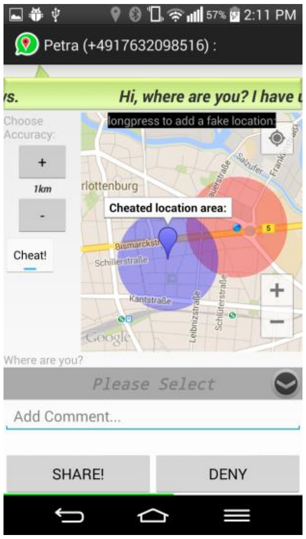
### *2.1.2 Contextual Sharing*

The users could share their situational context using two methods: selecting from the drop-down menu, or typing a message. In a messaging application used in the study of Iachello et al. [13], the users could type in the context menu the places they visited. To reduce the user overhead, we used a fixed set of menu items for Locate!. The items were selected based on a preliminary experiment that was conducted using an experiment sampling method [16]. This preliminary study aimed at identifying how various locations and situations affected the users' feelings. The feelings were reported using a location-based polling tool FlashPoll [17] at various times of the day on a six-point answer scale that measures anxiety [18]. We collected 62 reports from 15 participants during a four-day period. From these reports, we selected the context menu items for Locate! based on the most usual contexts that were reported as follows: *At School*, *At Home*, *At Work*, *Commuting*, *Out in the City*, or *Somewhere Else* (German: *In der Schule*, *Zuhause*, *Auf der Arbeit*, *Beim Pendeln*, *Unterwegs*, and *Woanders*).


Petra (+4917632098516) :

Hi, where are you? I have unfortunately sor

**Figure 1: Locate! gives visual feedback of the shared location.**


Petra (+4917632098516) :

Hi, where are you? I have

**Figure 2: Faked location or denying could be chosen instead of location sharing.**

## 2.2 Participants

To cover a large variety of participants, various methods were used to recruit, including billboard and online advertisements, and an online portal for participants. In total 22 participants between the ages 18 and 51 (median: 25.5) completed the study (65% females). Even though the sample size was rather low, it is still sufficient for statistical tests [19]. An incentive of 30€ was given after completing all the phases of the experiment. All the participants had finished at least a secondary education, and 38% had an academic degree. 24% of the participants worked or had worked in computer science or related field. The study required the participants to have a smartphone in active use, and therefore the users were mainly experienced smartphone users (1-3 years of experience 52%, >3 years of experience 38%). Most of the participants stated that they use smartphones hourly or more, with even the least active smart phone users using the device several times a day.

## 2.3 Test Procedure

The participants used Locate! during a seven-day period. During this time, in total 386 messages were sent to the participants, 352 of which were responded to. One participant had technical issues, and we left him out of the analysis.

### *2.3.1 Field Study*

To make the location requests as realistic as possible, we asked the participants to provide six contacts from their address books within the following categories: distant friend, boss, colleague, family member, close friend, and partner. Based on the social penetration theory [7], we expect closer relationships yielding to more accurate location disclosures.

To study the influence of the reason why location is requested, three categories of messages were created to justify the request. The *request categories* were a socially pleasant, *positive* message, such as “Hi, where are you? Would you like to go for a coffee?”, a socially unpleasant, *negative* message, such as “Hi, there is an issue we need to discuss face to face. Where are you?”, and a *neutral* “Hi, where are you?”, where no reason for the location request was given.

The participants received messages that were seemingly from each of the given requesters with the three different *request categories* during a seven-day period. The messages with the different *request categories* and requesters were randomly allocated to be received at various times of the day.

To verify what the feeling associated with each message type was, we asked the participants afterwards how comfortable they felt when receiving these messages. The pleasantness was measured on a continuous seven-point answer scale (Very unpleasant = 1 to Very pleasant = 7). A manipulation check showed a significant difference between the *request categories* confirming that the *positive* messages were perceived as more pleasant than *neutral* ones, and both as more pleasant than *negative* ones. Furthermore, the interpersonal closeness with each of the requesters was measured on a seven-point answer scale as adapted from Popovic et al. [20]. Based on the median of these measures we grouped the participants into users who generally feel close to others, and users who generally feel distant to others.

### *2.3.2 Assessment of Privacy Preferences*

For studying the users’ privacy concerns, we used a first version of a questionnaire which is currently being developed at our lab. The questionnaire is based on earlier works of Smith et al. [18], and Malhotra et al. [19], and contains thirteen items on seven-point answer scales anchored with “strongly disagree” and “strongly agree”. The questionnaire is being developed especially for measuring mobile users’ information privacy concerns. The questionnaire showed good internal consistency as a global measure (Cronbach’s $\alpha = .77$), and on the four subscales, namely *Access* (Cronbach’s $\alpha = .63$), *Security* (Cronbach’s $\alpha = .84$), *Risk* (Cronbach’s $\alpha = .70$), and *Purpose*, (Cronbach’s $\alpha = .84$).

To assess users’ disclosing behaviour, we measured how often each user changed the shared location to more accurate than the default accuracy. This percentage was used as a measure of willingness to share location.

## 3. RESULTS

Contrary to our assumptions and previous studies [8], [10], [11], neither the *request category* nor the requester influenced the willingness for disclosure. The Chi-square test shows a significant effect for the education level and privacy concerns: the participants with at least high school education had higher scores on the overall mobile users privacy than the ones with less education, $X^2(2)=6.36$, $p=.04$. Interestingly, level of education did not affect willingness to disclose location.

An ANOVA (Analysis Of Variance) showed that the participants who stated that they use some applications for securing their phones (app) from threats shared their location shared their location less often accurately compared with participants who did not use such applications (no app). $F(1,20)= 4.49$, $M_{app}=43.33$, $SD_{app}=30.10$, $M_{no\_app}=69.02$, $SD_{no\_app}=24.87$, $p=.047$. The users of security protective applications did not, however, score higher privacy concerns.

Regarding users’ privacy concerns an ANOVA showed significant effects for the subscale *Access*, which measures concerns regarding accuracy of personal information: participants scoring high on this scale were less willing to share their location compared to the participants scoring low. $F(1,20)=9.78$, $M_{low} = 49.46$, $SD_{low}=21.58$, $M_{high} = 24.27$, $SD_{high} = 14.71$, $p < .01$.

For the interpersonal closeness an ANOVA indicated that the participants with low closeness scores shared their location more accurately more often than the ones with high scores, $M_{low} = 46.85$, $SD_{low} = 22.57$, $M_{high} = 25.43$, $SD_{high} = 14.14$, $p = .02$. The users with low closeness scores feel generally close to others.

## 4. DISCUSSION

### 4.1 Individual Characteristics and Sharing

The individual characteristics such as privacy concerns seemed to dictate the participants’ location sharing behaviour more than who the requester was or the contextual variables. Concerning personal characteristics and demographical data, neither IT-experience nor age had an effect on either the willingness to share the location, or on privacy concerns. The level of education, however, seemed to influence one’s privacy concerns. The participants with higher education had more privacy concerns, suggesting that with education one gains some privacy consciousness. To study whether the level of education would also result in more privacy preserving behaviour, post-hoc analyses with respect to usage of mobile security applications and disclosing behaviour were carried out. There was no significant effects found, further confirming the earlier findings suggesting that the users’ privacy preferences are not in line with their actual behaviour [1], [2].

The users who score low on the "Access" scale tend to share their location more accurately compared to the more concerned users. This implies that at least some types of privacy concerns lead to a restricted location disclosure. When asked about whether they used applications for secure communication, most of the users either did not use such applications, or did not know whether the messaging apps they used were secure. A particular non-secure application was mentioned by two participants as an app that they use for secure communication, which can be seen as an indication of how unaware of the privacy and security risks the users can be.

The tendency to score high on interpersonal closeness increases the willingness to share location more accurately. This might imply that the people who feel close to others would find it more important to let others know exactly where they are. To test whether this also implies that the people who tend to feel close to others would have lesser privacy concerns, post-hoc analyses were carried out. These analyses showed no significant results, and further studies would be needed to verify this initial finding.

## 4.2 Requesters' Effect on Disclosure

One possible explanation for the surprising finding that neither the requester nor the *request category* influenced the willingness to disclose location could be that irrespective of our attempts to make the study as realistic as possible, the location requests were still not plausible enough. Also a lack of response to location disclosures might have resulted in the users not perceiving the subsequent requests as plausible. What might have further exacerbated the situation is that some requests might have not been meaningful for that specific context.

Some participants commented on the messages not being very credible when the context and the location request clashed. For instance, when colleagues or bosses sent location requests during a weekend, the participants sometimes responded by saying that work-related issues can also wait until the next working day. Other times the request was responded to with a friendly message, but later on commented that the request had seemed rather peculiar. Also, one participant commented that the location requests from her boss were written in a language that was more informal than what was normally used in the communication between them.

However, we have good reason to believe that, at times, the participants could relate to the received messages well and even genuinely believe that they came from the actual contacts. One participant commented: "For a moment my pulse went up when I received a message from my sister saying that something was wrong". Another one stated: "I wondered what kind of problem she was talking about, and how urgent [the issue was] and why she would need to know my location". Based on these comments, we believe that this work provides insight to location disclosure in a realistic setting; however, further studies are needed to confirm these results.

## 5. CONCLUSIONS

Our aim was at studying how different variables affect the location disclosure using a mobile application. The first results of the study showed that mainly the individual user characteristics influence the willingness to disclose. These include certain types of privacy concerns, as well as tendency to feel generally close to others.

While our intention was to have the setting as realistic as possible, we still made some compromises that might have resulted in an artificial setting. It is possible that even if the users could initially find the location requests genuine, some unrealistic requests or the lack of response to the location disclosures might have resulted in our application not being viewed as a normal messaging service.

A continuation study would need to be done in a setting where the participants use the application as a part of their normal communication. This would involve a significant amount of users who use a location sharing service on a daily basis.

## ACKNOWLEDGEMENTS

We would like to express our great appreciation to Dr. Rahul Swaminathan for reviewing this paper and for his helpful comments. This work is funded by the EIT project FlashPoll.

## 6. REFERENCES

[1] S. Spiekermann, J. Grossklags, and B. Berendt, "E-privacy in 2nd Generation E-Commerce : Privacy Preferences versus actual Behavior," in *ACM Conference on Electronic Commerce*, 2001, pp. 1–10.

[2] B. Berendt, O. Günther, and S. Spiekermann, "Privacy in e-commerce: Stated Preferences vs. Actual Behavior," *Commun. ACM*, vol. 48, no. 4, pp. 101–106, 2005.

[3] C. Jensen, C. Potts, and C. Jensen, "Privacy practices of Internet users: Self-reports versus observed behavior," *Int. J. Hum. Comput. Stud.*, vol. 63, no. 1–2, pp. 203–227, 2005.

[4] R. Gross, A. Acquisti, and H. J. H. Iii, "Information Revelation and Privacy in Online Social Networks ( The Facebook case )," *ACM Work. Priv. Electron. Soc. (WPES), 2005*, p. 11, 2005.

[5] L. Barkuus, A. Dey, and L. Barkhuus, "Location-Based Services for Mobile Telephony : a Study of Users ' Privacy Concerns Location-Based Services for Mobile Telephony : a study of users ' privacy concerns," in *Proceedings of the INTERACT 2003, 9TH IFIP TC13 International Conference on Human-Computer Interaction*, 2003, pp. 1–5.

[6] L. Palen and P. Dourish, "Unpacking 'privacy' for a networked world," *Proc. Conf. Hum. factors Comput. Syst. - CHI '03*, no. 5, p. 129, 2003.

[7] I. Altman and D. A. Taylor, *Social Penetration: The Development of Interpersonal Relationships*, vol. 75. 1973, p. 212.

[8] S. Consolvo, I. E. Smith, T. Matthews, A. LaMarca, J. Tabert, and P. Powledge, "Location disclosure to social relations," in *Proceedings of the SIGCHI conference on Human factors in computing systems - CHI '05*, 2005, p. 81.

[9] J. S. Olson, A. Arbor, J. Grudin, and E. Horvitz, "Toward Understanding Preferences for Sharing and Privacy," in *CHI '05 Extended Abstracts on Human Factors in Computing Systems*, 2004, pp. 1985–1988.

[10] S. Lederer, J. Mankoff, and A. K. Dey, "Who wants to know what when? privacy preference determinants in ubiquitous computing," *CHI*, p. 724, 2003.

[11] A. Khalil and K. Connelly, "Context-aware telephony: privacy preferences and sharing patterns," in *Methodology*, 2006, pp. 469–478.

[12] J. Y. Tsai, P. G. Kelley, L. F. Cranor, and N. Sadeh, “Location-Sharing Technologies : Privacy Risks and Controls,” *A J. Law Policy Inf. Soc.*, vol. 6, no. 2, pp. 119–151, 2010.

[13] G. Iachello, I. Smith, S. Consolvo, G. D. Abowd, J. Hughes, J. Howard, F. Potter, J. Scott, T. Sohn, J. Hightower, and A. Lamarca, “Control , Deception , and Communication : Evaluating the Deployment of a Location-Enhanced Messaging Service,” in *UbiComp 2005: Ubiquitous Computing*, 2005, pp. 213–231.

[14] 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*, vol. 13, no. 6. pp. 401–412, 2009.

[15] A. N. Joinson, C. Paine, T. Buchanan, and U. D. Reips, “Measuring self-disclosure online: Blurring and non-response to sensitive items in web-based surveys,” *Comput. Human Behav.*, vol. 24, no. 5, pp. 2158–2171, 2008.

[16] M. Poikela, T. Hirsch, and S. Möller, “Contextual Anxiety and its Effect on Perceived Privacy ,” Quality and Usability Lab, Telekom Innovation Laboratories, TU Berlin, Tech. Rep., in preparation.

[17] European Institute of Technology and Forschungsserie Digital Cities, “FlashPoll,” 2014. [Online]. Available: http://flashpoll.eu/.

[18] T. M. Marteau and H. Bekker, “The development of a six-item short-form of the state scale of the Spielberger State-Trait Anxiety Inventory (STAI).,” *Br. J. Clin. Psychol.*, vol. 31 ( Pt 3), pp. 301–306, 1992.

[19] H. Coolican, *Research Methods and Statistics in Psychology*, vol. 2nd, no. 1990. Hodder & Stoughton, 2009, p. 703.

[20] M. Popovic, D. Milne, and P. Barrett, “The scale of perceived interpersonal closeness (PICS),” *Clin. Psychol. Psychother.*, vol. 10, no. 5, pp. 286–301, 2003.