Which Cloak Dresses You Best? - Comparing Location Cloaking Methods for Mobile Users

Susen Döbelt
Cognitive & Engineering Psychology, Chemnitz University of Technology, 09120 Chemnitz, Germany
susen.doebelt@psychologie.tu-chemnitz.de

Johann Schrammel
AIT – Austrian Institute of Technology
Center for Technology Experience
Giefinggasse 2, 1210 Vienna
johann.schrammel@ait.ac.at

Manfred Tscheligi
AIT – Austrian Institute of Technology
Center for Technology Experience
Giefinggasse 2, 1210 Vienna
manfred.tscheligi@ait.ac.at

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the Owner/Author.

Copyright is held by the owner/author(s).
MobileHCI '17, September 4–7, 2017, Vienna, Austria
ACM ISBN 978-1-4503-5075-4/17/09.
https://doi.org/10.1145/3098279.3122138

Abstract
Location cloaking methods enable the protection of private location data. Different temporal and spatial approaches to cloak a specific user location (e.g., k-anonymity) have been suggested. Besides the research focusing on functionality, little work has been done on how cloaking methods should be presented to the user. In practice common location referencing services force the user to either accept or deny exact positioning. Therefore, users are not enabled to regulate private location information on a granular level. To improve the usage of location cloaking methods and foster location privacy protection, we conducted a user study (N = 24) comparing different visualized cloaking methods. The results of our lab study revealed a preference for visualizations using already known and well understood real world entities. Thus, the usage of simple and real world concepts can contribute to the application of cloaking methods and subsequently to location privacy protection.

Author Keywords
Location privacy; mobile location sharing; location cloaking; location obfuscation; user study.

ACM Classification Keywords
H.5.2. Information interfaces and presentation (e.g., HCI): User Interfaces; Screen design (e.g., text, graphics, color)

Introduction

User location data enables assisting services for mobile applications, e.g., resource finding, route planning and location-based gaming. However, location data conveys also sensitive information. Especially long-term and high resolution location data is a rich source of information that allows extracting behavioral patterns and individual lifestyle indicators. A possibility to support location privacy [8] is to enable users to control the release of location data on a granular level. Therefore, comprehensible user interface are needed to foster the usage of location cloaking approaches.

Related Work

Types of services with special relevance for location privacy aspects are applications where the user's location is visible to other users (location sharing) [5]. Particularly in the context of growing mobile use of social networking location sharing is getting more and more popular. Unfortunately, these services are not flexible enough to support different granularity [2] and therefore regulate private information flow. Instead the user is either to accept or deny exact position sharing. To deal with the inherent privacy problems of location sharing applications several approaches have been suggested.

A popular approach, build up on users' decisions on social appropriateness [2, 10], is sharing one's exact location with a defined set of contacts (e.g., Google maps share location functionality). The information is only visible to a trusted subset of 'friends` [16]. Another frequently suggested approach is to "blur", "cloak" or "obfuscate" the location information. These location cloaking methods can be classified into temporal and spatial approaches [7]. Temporal approaches blur location data by reducing tracking frequency, whereas spatial location cloaking methods enlarge an exact user location q into a cloaked region Q' so that it is impossible to reconstruct q from the region Q' [18]. Different methods can be used to construct this cloaked region, e.g. by randomly displacing a circle [15] or by using a real-world semantic region or replacing the exact position of an individual by a cloaked region containing several other users (k-anonymity, [9, 12]). K-anonymity was modified by different authors who considered user's preferences of private locations [6, 14]. Recent frameworks [1] suggest including further dimension of location privacy, such as activity (e.g., contextual information on transportation modes, tasks and activity) and identity (personal information).

Besides this work focusing on the functionality of cloaking approaches little work has been done on how cloaking methods should be presented to the user in the user interface [1, 9]. Tang [14, 15] studied user perspectives on location-aware social mobile applications. Results of 12 semi-structured interviews indicate that participants were concerned that other users' misinterpret their location data and derive wrong conclusions regarding the location, which might lead to unwanted social consequences.

Brush [4] studied user preferences of different cloaking methods using GPS data in a long-term experiment. Most of the 32 participants preferred "Mixing" (k-

anonymity) followed by "Deleting" (deleting data near home) and "Randomizing" (adding Gaussian noise to locations).

Above mentioned studies focus on user perspectives of location cloaking methods. To complement this work and support usage of cloaking methods, studies on user optimized visualizations are needed.

Research Questions

To address the lack of knowledge on user perspectives on cloaking methods, we performed a user study. We particularly aimed to investigate how location cloaking methods should be displayed. We wanted to investigate whether there are differences between the visualized cloaking methods with regard to a) user preference, b) comprehensibility and c) perceived locatabilty. Furthermore, we expected an influence of privacy ratings on preference for a location cloaking method.

Method

Study Design

To answer our research questions we conducted a within subject study, which compared visualizations of four location cloaking methods. The following location cloaking methods were selected in order to represent a broad range of spatial cloaking approaches: "Circle Method", "Landmark Method", "Spatial Units" and "One upon Others" (Figure 1):

- The "Circle Method" displays a circle with a given radius and random offset so that the true position of the user lies within the borders.
- The "Landmark" method uses a randomly chosen landmark displayed within the given radius as center of the cloaked region. This visualization was designed with respect to verbal descriptions of location information ("I`m close to…").
- "Spatial Units" cloak user's location by selecting a semantic unit based on the users' position. We use the city district as smallest cloaking unit.
- Finally, "One upon Others" equates to the k-anonymity method [8]. The visualization appeared similar to the "Circle Method" as circle on a map.

We presented real-scale paper mockups (printouts) of smartphones displaying maps with cloaked regions according to the different cloaking methods to the participants. The sequence of cloaking methods was randomized to avoid effects of sequence. To avoid influence of local geography knowledge three different user positions were used to visualize each cloaking method. To study influence of individual privacy concern participant's general privacy concerns were measured by Global Information Privacy Concern (GIPC) ratings [13]. Semi-structured interviews, questionnaires, rankings and estimation tasks were used to compare the four different visualizations.

Procedure

Study participants were welcomed and received a written introduction describing the general purpose of location sharing applications, the possibly arising data privacy issues and the possibility to obfuscate specific locations. Participants were asked to fill out a pre-questionnaire gathering demographic data, local geographical knowledge, experience with location sharing applications and general privacy ratings.

Next, study participants received printed material to illustrate the first location cloaking method consisting of

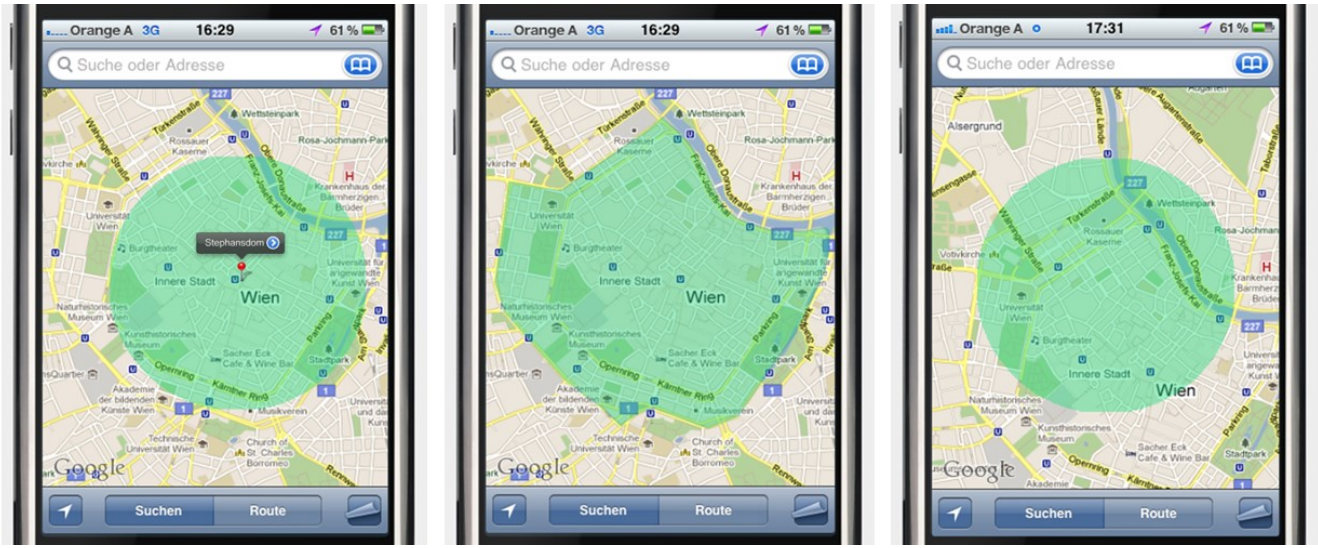

Figure 1: Example visualizations of the different cloaking methods: a) left: "Landmark" b) middle: "Spatial Units" c) right: "One upon Others" and "Circle Method"

a) a short description explaining the functionality of the cloaking method and b) three printouts, each showing a different city area using the location cloaking method.

After the participants studied the material carefully, they were asked to describe the presented cloaking method in their own words. These explanations were used to rate the comprehension of the presented location cloaking method. Afterwards emerging ambiguities were clarified by the study facilitator. Then participants were asked to think of advantages and disadvantages of the cloaking method and the visualization. Answers analyzed to generate further insights on underlying reasons for user's preference. Furthermore, participants were asked to estimate how accurately they could be located by others and what assumptions could be made by a location requester (locatability). This procedure was repeated four times with each of the different cloaking methods.

Finally, participants were asked to rank the location cloaking methods from "most preferred" to "least preferred" and whether they are willing to use location cloaking methods in general.

Participants

Our sample comprised N = 24 participants (12 female, 12 male) with an average age of 25 years (SD = 3.93). The majority of the participants were residents of the investigated city (92%), described their local geographical knowledge as "average" (50%) and were

not experienced with location sharing applications ("rare usage" 46%, "no usage" 33%).

Results

Preference for location cloaking method

On average the most preferred method was "Spatial Units" (*Mdn* = 1.83), followed by "Circle method" (*Mdn* = 2.10), "Landmark" (*Mdn* = 2.42) and "One upon other" (*Mdn* = 3.65). To test if the methods differ with regard to user preference a Friedman's test was computed. The analysis shows a significant effect ($\chi^2(3) = 27.895$, $p < .001$).

Bonferroni corrected signed-rank tests revealed one significant difference between "One upon Others" and "Landmark" ($p < .001$).To test if GIPC ratings have a significant effect on the preference for location cloaking method, participants were split by median into two groups (high vs. low GIPC ratings). Subsequently, a MANOVA was computed.

The factor privacy ratings had no significant effect on: Preference for "Landmark" ($p = .426$), "Spatial Units" ($p = .623$), "One Upon Other" ($p = .578$), and "Circle Method" ($p = .719$).

Table 1 below shows a summary of mentioned advantages and disadvantages of each method. "One upon Others" and "Landmark" received the most critique. "Spatial Units" and "Circle Method" received most positive feedback. "General disadvantages of cloaking" (e.g., in case of emergency or constrains of using Location Based Services) were mentioned frequently.

However, this was not directly related to a specific cloaking method and therefore we did not consider it for the comparison. Results of the post-interviews indicate that about two thirds of the participants (67%) are interested in using location cloaking. Users not interested in cloaking methods typically want to share their exact location or no location at all.

Circle	Spatial Units	One upon Others	Landmark
Disadvantages mentioned by participants (frequency)			
• misleading of others (9) • general cloaking disadv.(8) • circle inadequate (3) • other (6)	• general cloaking disadv. (10) • information leak on the move (5) • unaesthetic shape (4) • other (7)	• context dependent (10) • uncontrollable (9) • general cloaking disadv.(4) • other (7)	• misleading of others (12) • context dependent (5) • information unnecessary (4) • other (7)
Advantages mentioned by participants (frequency)			
• privacy enhancing (11) • context independent (5) • usable(5) • other (3)	• conceivable unit (9) • privacy enhancing (6) • self-explanatory (6) • other (8)	• idea of including others (8) • location accuracy (4) • other (7)	• guides orientation (9) • privacy enhancing (6) • similar to verbal descriptions (3) • other (3)

Table 1: Categorized statements and frequencies of method specific disadvantages, advantages

Comprehensibility

To determine a degree of comprehension, participant's verbal description of each method was rated with regard to their correctness on a three-point scale (*explanation correct* = 2, *explanation partly correct* = 1; *explanation wrong* = 0). Due to malfunction of audio recording the data of one participant was not available. "Spatial Units" was understood most correctly (M = 1.65) followed by "Circle Method" (M = 1.43), "Landmark" (M = 1.22) and "One upon other" (M = 0.87). To test differences in comprehensibility a repeated measures ANOVA was calculated. Results showed a significant difference ($F(3,66) = 4.561$; $p = .006$) between the cloaking methods. Post-hoc test using Bonferroni corrected paired samples t-test showed significant difference ($t(22) = 3.458$; $p = .002$) between the most correctly ("Spatial Units") and least correctly comprehended method ("One upon others".)

Perceived Locatability

On average the participants estimate how accurately they could be located by others as 2.49km for "Circle Method", as 2.30km for "Landmark", as 3.49km for "Spatial Units" and as 2.42km for "One upon Others". Due to missing sphericity of the data (Mauchly's test, $p < .001$) and missing normal distribution of a variable (Kolmogorov-Smirnov test, $p = .012$) a non-parametric Friedman's test was used. Testing the hypothesis that location cloaking method influences accuracy of perceived locatability showed no significant effect ($\chi^2(3) = 6.745$, $p = .080$).

Table 2 shows most likely location assumptions of a recipient expressed by participants. Participants mainly criticized the misleading effects of the landmark indicator when using the "Landmark" method. Furthermore, personal information about the cloaked user enables the requester to identify candidates for probable positions of the user.

Discussion

This study investigated how location cloaking should be displayed to users. Qualitative and quantitative data analysis showed the expected differences with regard to preference and comprehension. Users comprehend and prefer "Spatial Units" over "Circle Method", "Landmark", and "One upon Others".

Circle	Spatial Units	One upon Others	Landmark
Assumption (frequency)			
• center (12) • anywhere (5) • anywhere, with personal information probable positions could be derived (3) • other (4)	• anywhere (14) • anywhere, with personal information probable positions could be derived (7) • at specific location (3)	• anywhere (9) • center (7) • anywhere, with personal information probable positions could be derived (4) • other (4)	• at the landmark (15) • anywhere (7) • anywhere, with personal information probable positions could be derived (2) • other (2)

Table 2: Categorized statements and frequencies of method specific location assumptions of a requester

Concluding "One upon Others" was evaluated significant worse than all other compared location cloaking methods. We think this result is caused by difficulties with comprehensibility due to the relative complexity of "One upon Others". Cognitive effort is needed to estimate and predict cloaking behavior of this method and implications of reported advantages and disadvantages led to a perceived lack of control regarding cloaking intensity.

In contrast to our results the results of Brush [2] indicate a preference for the k-anonymity method ("Mixing"). We think these differences are caused by the following two factors: First, the sample of methods studied by Brush consisted of rather advanced cloaking methods. Simple approaches like our "Circle Method" were not included. Second, according to our perception study materials used by Brush were designed for explaining the functionality of the compared cloaking methods and not optimized for everyday usage. Therefore, we conclude location cloaking methods should hide their complexity on a user interface design level no matter which cloaking algorithm is applied.

Participant's quantitative estimations on accuracy of locatability showed in contrast to our hypotheses no differences. Therefore we conclude the participants perceived the cloaking performance of the compared methods similar. Qualitative statements indicate participants want to avoid "misleading of others". This is in line with the conclusion of Tang [14]. Potentially misleading location hints (e.g., landmark pins) should be avoided or carefully designed especially in a social community context.

Acknowledgements
Research reported in this paper has been partially funded by the European Commission project OPTIMUM (H2020 grant agreement no. 636160-2)

In contrast to our hypotheses general privacy ratings had no significant effect on location cloaking preference of our study participants. Both, privacy concerned and unconcerned users prefer simple location cloaking methods.

Limitations and Future Work

For our lab study we choose the GIPC scale to efficiently assess a general level of privacy concerns. To study the effect on a more detailed level future work should also consider multiscale and more specific measurements [for an overview see [11] such as CFIP, IUIPC or MUIPC [17].

Furthermore, the validity of our results is limited due to the lab environment and the specific context of location sharing applications we choose. Last was motivated by our project background focusing on the usable design of privacy preserving community applications. However, future work should investigate visualizations of location cloaking in the wild [2] to research long-term and effects of personal relevance to obfuscate a specific location. The choice for certain obfuscation visualization will very likely vary depending on the individual situation and therefore motivation for location privacy protection.

Conclusions

In our study users appreciated the usage of rather simple visualizations ("Spatial Units" and "Circle Method"), respectively visualization that use concepts related to already known and real world entities. Based on these results we propose that location cloaking methods should hide their complexity on a user interface level by using real world concepts.

References

1. Andersen, M.S., Kjargaard, M.B., Grønbæk, K. 2013. The SITA principle for location privacy—Conceptual model and architecture. In *Privacy and Security in Mobile Systems (PRISMS),* IEEE, 1-8.
2. Barkhuus, L. 2012. The mismeasurement of privacy: using contextual integrity to reconsider privacy in HCI. In *SIGCHI Conference on Human Factors in Computing Systems,* ACM, 367-376.
3. Beresford, A., Stajano, F. 2003. Location Privacy in Pervasive Computing. *IEEE Pervasive Computing*.
4. Bernheim Brush, A.J., Krumm, J., Scott, J. 2010. Exploring end user preferences for location obfuscation, location-based services, and the value of location. *Conf. on Ubiquitous computing*, ACM.
5. Chow, C., Mokbel, M.F. 2009. Privacy in Location-based Services: A System Architecture Perspective. *Sigspatial Special*, 1(2), 23-27.
6. Damiani, M.L., Bertino, E., Silvestri, C. 2010. The Probe framework for the personalized cloaking of private locations. *Transactions on Data Privacy*, 3(2), 123-148.
7. Duckham, M., Kulik, L. 2006. Location Privacy and Location-Aware Computing. In *J. Drummond, Dynamic & Mobile GIS: Investigating Change in Space and Time*, 3, Boca Raton, FL.: CRC Press.
8. Gruteser, M., Grunwald, D. 2003. Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking. In *Conference on Mobile systems, applications and services*. ACM, 31-42.
9. Henne, B., Kater, C., Smith, M., Brenner, M. 2013. Selective cloaking: Need-to-know for location-based apps. In *Privacy, Security and Trust (PST), 2013 Eleventh Annual International Conference on Privacy, Security and Trust*, IEEE, 19-26.
10. Nissenbaum, H. 2009. *Privacy in context: Technology, policy, and the integrity of social life.* Stanford University Press.
11. Preibusch, S. 2013. Guide to measuring privacy concern: Review of survey and observational instruments. In *International Journal of Human-Computer Studies*, 71(12), 1133-1143.
12. Sheehan, K.B. 2002 Towards a Typology of Internet user and Online Privacy Concerns. *The Information Society*, 18 (1), 21-32.
13. Smith, H.J., Milberg, S.J., Burke, S.J. Information privacy: Measuring individuals concerns about organizational practices*. MIS quarterly*, 20(2).
14. Tang, K.P. 2010. *Sometimes Less is More: Multi-Perspective Exploration of Disclosure Abstractions in Location-Aware Social Mobile Applications.* Doctoral Thesis, HCII, Carnegie Mellon University.
15. Tang, K.P., Hong, J.I., Siewiorek, D.P. 2011. Understanding how visual representations of location feeds affect end-user privacy concerns. In *Conference on Ubiquitous computing*, ACM.
16. Wilson, S., Cranshaw, J., Sadeh, N., Acquisti, A., Cranor, L.F., Springfield, J., Jeong, S.Y., Balasubramanian, A. 2013. Privacy manipulation and acclimation in a location sharing application. In *ACM international joint conference on Pervasive and ubiquitous computing*, 549-558.
17. Xu, H., Gupta, S., Rosson, M.B., Carroll, J.M. 2012. Measuring mobile users' concerns for information privacy. In Joey, F.G. (Ed.), *International conference on information systems.*
18. Xue, M., Kalnis, P., Pung, H. 2009. Location Diversity: Enhanced Privacy Protection in Location Based Services. In *4th International Symposium on Location and Context Awareness*.
19. Yiu, M.L., Jensen, C.S., Huang, X., Lu, H. 2008. Spacetwist: Managing the trade-offs among location privacy, query performance, and query accuracy in mobile services. In: *International Conference on Data Engineering.* IEEE, 366-375.