# Privacy in Location-Based Services, Concern vs. Coolness

Louise Barkhuus

Department of Design and Use of IT,
The IT University of Copenhagen,
Rued Langgaards Vej 7, Copenhagen 2300
Denmark
`barkhuus@it.edu`

**Abstract.** New location-based technology attempts to facilitate people's privacy but developers have little knowledge of how users are in fact concerned about their location privacy. I present two case studies indicating that users are initially concerned with their privacy, but when actually using location-based services, users discontinue to have the same level of concern. The paper concludes by addressing three issues of design that should be of concern to designers of location-based services.

## 1 Introduction

Privacy, in relation to location-based and mobile services, is in most cases considered essential and an issue where 'more is better'; the more privacy the designer can provide, the better it is for the user. Developers often assure the users that their specific application maintain their privacy and that no data will be shared with other parties [8]. The few settings where location services are already implemented, providers go to great lengths to ensure that people's private data is not shared or compromised. AT&T for example, offers their customers to locate each other but when one user asks for another's location the other is sent a text message to indicate that they have been located [1]. In many cases this high level of privacy is viewed by the provider to be an assuring factor for the user and it is applied to prevent concern from users. In this position paper I present data gathered through two case studies investigating issues and social dynamics of users' interaction with location-based services. Both studies show trends of users' initial worry about their privacy when presented with location-tracking applications; however, when actually using the services, users find them less threatening and accept them to a much higher degree than at first indicated.

The goal in this position paper is first of all to present novel findings and second to discuss the implications of these findings. By framing the findings into a larger understanding of state-of-the-art as well as future location-based services, the findings should provide better premises for design as well as future research in the area of location-based systems.

## 2 Case Studies

The two case studies were not initially designed to focus on users' concern and interactions in relation to location *privacy*, but after analyzing the results, it was clear that privacy was a central issue for the studied location-based applications. The results presented here are therefore previously unpublished, but related work from the same studies can be found in [2, 3, 4], which also have more detailed description of the method.

### 2.1 Method

The first case study used an experimental set-up with 23 users using 'imaginary' location-based services added to the participants' mobile phones throughout a week. They reported in a written fill-in journal (with room for extra comments) each night how, and to which degree, they had used the services throughout the day. The experiment was supplemented with interviews of six of the participants, pre-experiment and post-experiment.

The second case study was carried out in a campus environment with actual implemented location-based applications available to students (as well as researchers, lectures and visitors). The data was gathered in three ways: by observation of use in the campus setting, by questionnaire data from 35 students and finally open-ended qualitative interviews with 12 students. Most of the data reported in this paper are from the interviews. The students were mainly seniors, but four of them were freshman students participating in a seminar on future ubiquitous computing technologies. This seminar involved creation of a scenario of the campus of the future.

The setting was University of California, San Diego, where a set of context-aware applications are employed in the system of Active Campus. The applications include location tracking of fellow students and teachers and location dependent message services. A more detailed description can be found in [6]. The students can use it for messaging their peers and TA's as well as locating all users that have signed up (the only requirement is a UCSD email address). The individual user can set their profile to 'visible to all', meaning that everybody accessing the system can pinpoint their precise location on campus, 'visible to only buddies', meaning that they can only be located by the users they have accepted as 'buddies' or finally as 'invisible'.

## 3 Users' Concern for Privacy

Much of the data from the interviews indicate that users are fairly concerned with their own privacy when presented with location-based services. One participant from the first case study was asked what she would think of a service that would located her pre-defined friends on her mobile phone and that they could then also locate her[1]. She replied:

---

[1] It should be noted that this case study was carried on before any mobile phone provider offered the previous mentioned location tracking service.

> I don't know, because I don't think I would want my friends to be able to see where I am, not that I would be doing something bad. I guess it just depends. I think it would be good if I walk home late at night a lot, and there's a way to turn it on when I'm scared ...But I don't...still don't think I want people to see where I am.

Another participant from the same study said after the interviewer asked: "And you don't necessarily want to locate your friends either?"

> No, because I can just call them up and say "hey, where are you".

The latter participant hereby acknowledge that mobile phones have the services she needs and that she was generally content with present technology. This theme was apparent throughout the first case study; only one of the six interviewees thought that his/her present mobile phone should have more services such as the location-based service or access to wireless internet.

Most of the participants from the first case study mentioned that the potential location-tracking service should provide the user the possibility to turn it off. This feature is of course essential but many participants request a possibility for easy, instant turn-off such as disabling on an hourly basis. One student uses the example of Christmas present shopping, where she would not want her boyfriend to know where she was. She is not doing anything 'bad', she just wants to be anonymous for a short while.

The second case study revealed related findings but participants were less concerned with the identity of the people locating them. This is very likely due to the closed environment where the actual location system is implemented but could also be due to the closed nature of the campus environment that 'surrounds' the study; the interviews took place at campus in the participants well-known environment and the location service in question only worked in this environment. One participant, who did not use Active Campus, for example, views the services as practical but could also see himself as an intruder:

> I think it would be most useful for locating TA's and stuff. Like if I have a question and there is nobody in the lab...Picking on my friends would be fun...I can think of things like that...

Instead of viewing the location tracking as an invasion of his own privacy, he realizes that he can overstep boundaries of his friends.

In general the participants from both studies expressed concern but they were often able to see the advantages of location services as well. Two of the six participants in the first case study claimed that they would never use the location tracking services because they would not like to be traced themselves. However, none of the participants in the second case study had such hard claims. Some of them, however would never set themselves to 'visible to all'.

## 4   Actual Use of the Services

The first Case study traced the use of 'imaginary' services. This was due to our wish for early pre-prototype feedback in relation to context-aware services. At

present time (and at the time of the study), context-aware services are still rare and require a thorough infrastructure such as a location tracking wireless network. We therefore briefed the participants about six new services (four of them location based) that were 'now installed' on their mobile phones and let them use it for a week. The participants used the services quite a lot and expressed satisfaction with them by the end of the week. Three of the users did now want to use any of the location tracking services but the rest of them used all of the services at least once. The location-based services were used 1.3 times a day on average with some users being high level users (up to 5 time a day) and others not using the service at all. The participants who used the services often also found them useful. A correlation of .54 was found between if the user stated it to be useful and the number of times it had been used during the week. We also found a slight correlation of .31 of the participants' rating of usefulness and if they felt the location-based service invaded their privacy. The more useful they thought the service was, the more invading did they also find it.

In the second case study, use was not measured to the same detail as in the first study. Similar to findings by Colbert [5] we found that participants were willing to give up large amount of information about their location to a preselected but also broad group; three of the interviewed users of Active Campus had their profile set to 'visible to all' and the others were not opposed to revealing their location information to their 'buddies'. Their actual use however, was limited to locating TA's when they needed to ask class related questions and then chatting with other students. Some of them expressed how 'neat' it was that they could see where the ones they talked to were located. Although other research shows that the *inquirer* of a personal question such as ones location is the greater determinant to if the person will answer the question, than for example the social situation [7], our results indicate differently. Our participants in the second case study use a physically limited application and the potential enquirers very likely have some relation to the campus environment; this is likely the reason that some of the users do not worry about letting all possible users see their location. Another factor for the participants in the second case study is the positive impression that they express by using the locator; they find it 'cool' that they can see the actual location of their peers (and even unknown people). This coolness factor is likely to remove some of the concern for their own privacy.

Some users of new technology are surprised of how much information is passed on through interactive services. One girl from the second case study explained that she had been very distressed when one of her not-so-close acquaintances had asked if she had enjoyed her trip to the gym the previous day. She had set her instant messenger profile to 'At the gym' and he was on her list of 'buddies'. She explained that although that was to expect when having a large and fairly unlimited buddy list on her instant message program, she felt it to be a violation of her privacy. She was therefore not very positive towards the locator that she could use, but also phrased that she would need to get use to such technical possibilities. One of the consequences of the technological possibilities is that

users will slowly have to reevaluate the personal information that is available to others; in many cases this will not be apparent before the actual services are implemented and in use. It is our duty as researchers and designers to provide enough information to people about what and how personal information is displayed. Only this way can we prevent people from bad experiences of realizing how data that was preferred to be kept private, in fact are not so.

## 5 Factors for Design

As stated in the introduction, in relation to location-based services, privacy is often approached as more is better. This means that commercial services assure potential users that their privacy is safe and that their data will not be shared with others. The problem is, just as with internet based services, the common user have no way of actually verifying what is being done to their personal data. Even with a contract between user and service provider, the data can potentially be used for example in criminal court (examples of this have already been seen in Denmark); in the near future, the telephone service providers will be offering services based on location information, no matter if the user want the service or not. I now present three essential design issues, issues that arose from the two case studies and their findings.

As designers and researchers, it is important that we consider these potential services as inevitable technological development and it is then our goal to bridge the gap between users' understanding of what technology is capable of and what is useful for them. One of the obvious implications for design is the essential need for real-time information about the user's level of privacy in a specific situation. For users to accept the services they must know who can and especially who cannot see their location. It was evident from the two case studies that concern was prompted by uncertainty of the identity of the inquirers and that less concern was expressed in a fairly closed environment (despite UCSD's users exceeding a potential of 27000 students and employees).

Second, location-based services should enable short term deactivation. What worried the participants was also specific situations of shorter time-span. They could think about times where they would not want to be tracked, even by close family or friends. Some also requested to have a service that was only available in certain situations such as when she had to walk home alone at night. One way of making sure users will accept these services is than to make sure it is possible to turn off and inform the user when it is turned on or off.

Finally, as the case studies indicated, location-based services have greater potential for adoption in closed or at least limited environments. Despite the potential 27000 users, the services in the second case study were perceived less threatening for the participants, very likely due to the fact that they know there is a limit. Another factor could be that it is a non-commercial service and it is not likely that the data will end up in commercial environments. Services depending on location could therefore be restricted to closed settings, either physical (such as the UCSD campus) or user groups (for example co-workers). This way, the

users would have a greater sense of control and knowledge of who potentially will know their location.

## 6 Conclusion

I have in this paper presented finding of how location-tracking initially raises concern for privacy but that in an actual situation and in a fairly closed environment, privacy becomes less of a concern. It should be noted that the results presented here are drawn from initial analysis of two studies that reflects on privacy in location. The results should be viewed with its limitation such as the fairly small number of participants and the fact that the studies did not focus on privacy initially. Although the location-based services studied here were mostly exemplified by services locating people, the findings can be considered relevant for other types of location-based services as well. Services such as location-based advertising, mobile location-tracking for work environments as well as object-locating services can be considered alongside the examples presented here.

When developing location-based services it is essential to balance the design between what technology can offer and what users are willing to accept; however, users need guidance to determine if the service is acceptable or not, they often find services to be neat and do not realize what data they are revealing. Only by providing adequate information to the user about what location data is measured, stored and used later can the user make an informed decision of how and when to use the service.

## References

1. AT&T. At&t friendfinder. www.attwireless.com, June 2004.
2. L. Barkhuus and A. K. Dey. Is context-aware computing taking control away from the user? three levels of interactivity examined. In *Proceedings of UbiComp 2003*, Seattle, Washington, 2003. Springer.
3. L. Barkhuus and A.K. Dey. Location-based services for mobile telephony: a study of users' privacy concerns. In *Interact 2003*, Zurich, CH, 2003. ACM Press.
4. L. Barkhuus and P. Dourish. Everyday encounters with context-aware computing in a campus environment. In *To Appear in Proceedings of UbiComp 2004*, Nottingham, UK, 2004. Springer.
5. M. Colbert. A diary study of rendezvousing: Implications for position-aware computing and communications for the general public. In *Proceedings of GROUP '01*, pages 15–23, Boulder, Colorado, 2001. ACM Press.
6. W. G. Griswold, P. Shanahan, S. W. Brown, R. Boyer, M. Ratto, R. B. Shapiro, and T. M. Truong. Activecampus – experiments in community-oriented ubiquitous computing. Paper CS2003-0750, Computer Science and Engineering, UC San Diego, June 2003.
7. S. Lederer, J. Mankoff, and A. K. Dey. Who wants to know what when? privacy preference determinants in ubiquitous computing. In *Proceedings of CHI 2003*. ACM Press, 2003.
8. E. Snekkenes. Concepts for personal location privacy policies. In *Proceedings of Mobile Commerce*, pages 48–57, 2001.