5-2012

User perceptions of privacy risks regarding location-based services

Dalibor Kostic
Vienna University of Economics and Business, kosticd@gmx.at

Matthias Kollin
Vienna University of Economics and Business, h0651807@wu.ac.at

User perceptions of privacy risks regarding location-based services

Dalibor Kostic
kosticd@gmx.at
Vienna University of Economics and Business

Matthias Kollin
h0651807@wu.ac.at
Vienna University of Economics and Business

Abstract
Location-based Services (LBS) are widespread nowadays and with the rise of smartphones and other mobile-devices they are expected to be used in ever more applications by ever more users. There are clear opportunities this technology provides, nevertheless there are always privacy concerns when it comes to the identification of an individual's location. This paper provides an overview of user privacy risks regarding LBS. Based on a privacy taxonomy, it shows the gaps that exist in the literature, which could be of interest in further research to gain an even better understanding of privacy concerns of users and as a result their willingness to use LBS.

Keywords
Privacy, Location-Based Services, Risks, User Perceptions, Collection, Unauthorized Secondary Use, Improper Access, Errors

1. Introduction
The use of location-based-services (LBS) is on the rise. Through the vast distribution of smart phones and other mobile-devices there are more and more users who are using LBS (Gartner, 2011).The applications of such services are manifold, but bear also a threat potential. The privacy dimension regarding the use of LBS on mobile devices is currently an important topic and has been evaluated by several researchers. See e.g. Barkhuus and Dey (2003), Perusco and Michael (2007), Minch (2004).
These and other researchers have tried to shed light on the topic from different perspectives, which is important to understand the current academic atmosphere towards privacy concerns of users regarding LBS and the use of LBS.
The future development of the user adaption of LBS is said to be dependent on the perceived usefulness and the privacy concerns of users towards LBS (Barkhuus & Dey, 2003). People are concerned because the implications of the introduction of new LBS applications are not very well known and may pose a threat to them. To advance the research in this area will help to understand the user perceptions of privacy risks as a whole but also with focus on LBS.

If we look at Apple's iPhone (Apple, 2011) or smartphones from different producers with Android OS (Android, 2011), it is clear that apps are one important reason for the spread of these devices. These apps can make life convenient, more entertaining and help in everyday work. To use the full potential many apps need to use user's location (mostly GPS); otherwise such apps have limited or no functionality. But also social media apps provide the possibility for users to share their location with others (e.g. Facebook, Google latitude). From our own experience and surrounding we suppose that through the use of these modern devices with LBS, more privacy issues will occur and should be discussed. Thereby it is not only important to have a look at the technological perspective, but foremost at the psychological perspective, where the user plays the essential part.
The aim of this paper is a literature review of the current status-quo of perceived privacy risks of LBS from a user perspective. We used a privacy taxonomy, which we introduce later in the article, to analyze the literature along four privacy concern dimensions, 1) *collection*, 2) *unauthorized secondary use*, 3) *improper access*, 4) *errors*. We seek to find gaps in the current research literature to provide impulses for future work on the topic. We focused on papers that have been published at conferences in the last ten years and work that has been cited in these published papers.
We define the research methodology for finding the material we used for the analysis in chapter 2. In chapter 3 we discuss the used privacy taxonomy that we used as a basis for our literature review. The actual review and analysis of the material is conducted in chapter 4.
Finally, we will conclude with our findings and the possible gaps in the current literature on the topic in chapter 5.

2. Research methodology

We conducted our search for suitable papers in a structured way. First we defined keywords for the search query in a database or catalogue. After researching synonyms and associated terms, we decided to go with the key words "privacy", "security", "concerns" and "location based services". The combination of those keywords narrows the scope of search results and helps to define a rather specific research area. The combination of keywords was realized through use of Boolean-operators (AND, OR and NOT). Work that has been cited in these selected papers was also included into this literature review.

The keyword combinations we used to find our material were:

- privacy AND concerns AND "location based services"
- privacy AND security AND issues AND "location based services"

Besides the papers that delivered the content for our analysis, we tried to find a proper generic taxonomy of privacy on which we ground the structure of this review. Therefore a search for taxonomies was conducted. For finding proper results we choose the keywords "taxonomy", "privacy".
The keyword combination we used to find privacy taxonomies was:

- privacy AND taxonomy

Next we defined where we wanted to conduct the search with the predefined keywords. We chose to use Google Scholar as search engine as it was said to "[…] become an excellent free

tool for scholarly information discovery and retrieval" (Jacsó, 2005). Since then Google Scholar has indeed become a respectable source for scholarly information.
As LBS are a rather new topic we decided to only consider relevant work from the last ten years. We scanned through various papers that were the result list of our Google Scholar search and determined the quality of the papers based on the outlet (published conference proceedings, journal, etc.). In the end our review was mainly based on conference papers, which again reflects the novelty of the topic.
Which papers we picked was also influenced by the number of times a paper has been cited by other academic researchers up to now. In our decision we took into account, that older work has usually been more often cited than newer ones. The information about citations and published year is shown very transparent by Google Scholar and indicates, to some extent, the relevance of that paper to the academic world. We compared the number of citations of our found work with the *Thomson Reuters' Essential Science Indicators database, 1 January 2000-31 December 2010* (Times Higher Education, 2011). This database shows the average citations of papers of certain scientific fields from 2000 to 2010. Only papers have been selected in the end that had a citation count above the average presented in this database.
It must be noted that this database uses only citations of journal articles and reviews.

3. Privacy taxonomy

We want to use a framework or taxonomy which is the basis for our reasoning about the current literature. As our topic deals with privacy concerns towards LBS we picked a generic privacy taxonomy that works on a meta-level. The taxonomy we chose provides the categories or dimensions on which we analyze, compare and categorize the selected literature. Through this approach of arranging literature we want to find the "blind spots" of current academic literature and want to show where future research can close those gaps. The generic privacy taxonomy by Smith et al. (1996) tackles privacy concerns along four different dimensions: 1) *collection*, this concern is about the collection and storage of extensive amounts of personally identifiable data in databases, 2) *unauthorized secondary use (internal and external)*, that concern deals with the information that is collected for one purpose but then is used for another, secondary purpose, 3) *improper access*, expresses the concern that data about individuals are readily available to people not properly authorized to view or work with this data, and finally 4) *errors*, depict the concern that protections against deliberate and accidental errors in personal data are inadequate.
To reinforce the credibility of this privacy taxonomy we want to present a second taxonomy by Solove (2006). This taxnomy analyses privacy along rather similar dimension. That is 1) *information collection*, 2) *information processing*, 3) *information dissemination* and 4) *invasion*. The meaning of the dimensions of this taxonomy is overlapping to a great extent with the dimensions presented in the first taxonomy. For the analysis that we conducted we used the notation of the taxonomy by Smith et al, as this is an older and therefore more attested taxonomy. It must be noted that the dimensions of this framework not necessarily reflect a complete picture rather then a picture that copes with the "most central dimensions" (Smith et al., 1996) of user privacy concerns. The second taxonomy emphasizes and reconfirms the dimensions of the older taxonomy, which assures that the dimensions chosen for our analysis are reliable.

4. Analysis

The selected scientific material was analyzed and set into context of our work.
The analysis is divided into the four dimensions mentioned in the previous chapter. In every chapter the literature that fits into that very dimension is discussed.
The table bellow shows the four dimensions of the privacy taxonomy including the dedicated references for each dimension.

Collection (4 articles)	**Unauthorized secondary use (2 articles)**
Barkhuus, L., & Dey, A. (2003). Location-Based Services for Mobile Telephony: a study of users' privacy concerns Minch, R. (2004). Privacy issues in location-aware mobile devices. Clarke, R. (2001). Person-location and person-tracking: technologies, risks and policy implications Xu, H., & Teo, H.-H. (2004). Alleviating Consumer's Privacy Concerns in Location-Based Services: A psychological Control Perspective	Barkhuus, L., & Dey, A. (2003). Location-Based Services for Mobile Telephony: a study of users' privacy concerns Xu, H., Teo, H.-H., & Y., T. C. (2005). Predicting the adoption of location-based services: The role of trust and perceived privacy risk
Improper access (6 articles)	**Errors (2 articles)**
Lederer, S., Mankoff, J., & Dey, A. K. (2003). Who Wants to Know What When? Privacy Preference Determinants in Ubiquitous Computing Toninelli, A., Montanari, R., Lassila, O., & Khushraj, D. (2009). What's on Users' Minds? Toward a Usable Smart Phone Security Model Tsai, J. Y., Kelley, P. G., Cranor, L. F., & Sadeh, N. (2010). *Location-Sharing Technologies: Privacy Risks and Controls* Barkhuus, L., Brown, B., Bell, M., Hall, M., Sherwood, S., & Chalmers, M. (2008). From Awareness to Repartee: Sharing Locating within Social Groups Perusco, L., & Michael, K. (2007). Control, trust, privacy, and security: evaluating location-based services Anthony, D., Kotz, D., & Henderson, T. (2007). Privacy in Location- Aware Computing Environments	Junglas, I., & Spitzmüller, C. (2006). Personality Traits and Privacy Perceptions: An Empirical Study in the Context of Location-Based Services Perusco, L., & Michael, K. (2007). Control, trust, privacy, and security: evaluating location-based services

Table 1: Selected Literature assigned to the four dimensions of Smith's privacy taxonomy

4.1 Collection

The collection of data is an important dimension regarding privacy concerns of persons. LBS require a huge amount of location data that is collected and stored so that users of LBS applications can use services that derive their content based on the collected data. Users are concerned about this collection of data and Barkhuus and Dey (2003) conducted a study where they used the distinction between two kinds of LBS services: *location-tracking* and *position-aware* services. The difference in those services is that location-tracking services rely on third parties that track a persons' location therefore collecting data about a person's location. Position-aware services use the location knowledge of a person's device. So there is another form of data collection incorporated. The study shows that people are more concerned about their privacy when using location-tracking services, rather than position-aware services. A rather similar notion is presented by Minch (2004), who differntiates between *internal* and *external* determination of a mobile device location. Though with internal determination the GPS system is used, which is maintained by the U.S. government, the user's mobile device is just a receiver of information and can thereby be seen as independent of a third party. This work also states that "[…]the privacy issues raised in location information collection are relatively minor, as there is little potential for abuse until that information is retained, used, or disclosed in some way" (Minch, 2004). He also depicts the dimension of information retention, which deals with the following questions: where is the collected data stored?, how long is the collected data stored?, and how securely is the collected data stored? These are all questions that could have an important impact on the perception of users' privacy risks when using LBS. How long data is stored defines the usage possibilities of the location information. Minch mentions that "long term tracking and pattern recognition" (Minch, 2004) could be a result of a long-term storage policy. This notion is also emphasized by Clarke (2001), as he also gives examples of risks associated with long-term stored location information. He explains that the dangers of location tracking technologies lie in, e.g. "the discovery of individuals' behaviour patterns, thereby enabling matching against pre-determined patterns. This can be sued by the State in order to generate suspicion, and by the private sector to classify the individual into micro-markets and thereby to manipulate consumer behaviour" (Clarke, 2001).

Another aspect is added by Xu and Teo (2004). They explain that not only the direct capture of location through mobile devices is a concern, but also the storage and combining of historical location data with other personal information. Users feel observed by some unknown party if they don't know who and how their location information is used. This may create conditions of stress and anxiety. These concerns might be lower if users have a technological solution to control their own LBS information.

4.2 Unauthorized secondary use

The dimension *unauthorized secondary use* deals with any kind of secondary use of data that has been collected for another purpose. E.g. a person thinks LBS data was collected for providing an LBS service properly. The mobile phone service provider uses this data not only for providing an LBS service but uses it also for marketing issues. This secondary use was not authorized by the user and is also not intentionally wanted, which leads to a privacy risk. A main role plays trust, which users need to have in order to exploit the full bandwidth of services. Barkhuus and Dey (2003) also address this issue in their work. Another work that presents similar results is by Xu et al. (2005). They describe the concerns regarding the collection and dissemination of consumer

information by service providers and merchants. Therefore a study was conducted to examine the effects of third party privacy seals, P3P (Platform for privacy preferences project) compliance and device-based privacy enhancing features on consumers trust beliefs and privacy risk perception. The authors mention the concept of a social contract, which means that users are willing to disclose personal information if they get certain benefits as long as they trust the company that provides this benefits. The results show that through users trust beliefs their privacy risk perceptions can be mitigated and make it easier for them to disclose their location information. Also if the provider joins a third party seal program and if devices have privacy enhancing features, consumers trust beliefs can be increased. The reason for this is the level of enforcement provided by e.g. third party assurance. On the other hand if the bonus lies only on the user side, the perceived privacy risk is higher, this could be examined for P3P compliance. Although privacy enhancing features give users a greater control and more autonomy, which would lead to lower privacy invasion risk, as stated in (Xu & Teo, 2004), it is different for P3P, because it provides little assurance of control to consumers.

4.3 Improper access

Through their mobile devices users access different services and create a great amount of data. This data is in many cases required, but also users require knowing that their data is only accessed by people or services, which are authorized to do so. The concern of improper data access goes hand in hand with collection of personally identifiable data. Several authors address these issues and try to find reasons for the concerns users have with LBS from this perspective.

There is a connection of the term *improper access* and control. The selected literature for this chapter deals to some extent with control possibilities for users regarding the amount and granularity of location information exposed. If users cannot set the level of location information detail they want to share, then people, who are not supposed to, could improperly access that location information. The ability to control privacy settings is therefore an important aspect of this dimension.

Lederer et al. (2003) developed an interface for managing personal privacy and analyzed the importance of the factors of the inquirer's identity and user situations. The elements included in the questionnaire of the study were a mobile phone that was able to automatically determine the users' location and activity. Remotely another person (e.g. friend) could collect the users' information. Mobile phone users could choose what information they want to show to whom. Therefore two different situations were possible (working lunch and social evening) and four inquirers (spouse, employer, stranger, merchant). The study shows that the identity of the information inquirer is the stronger determinant. If the inquirer is a stranger, users are less ready to provide information. The situation is an important determinant if the inquirer is the employer. This research result is reinforced by the work of Toninelli et al. (2009), which also conducted a study regarding this topic. They state that willingness of people to share location information with someone else is depending on the relationship to the opponent. People want to have control about who has access to their location information. If people are not able to set the degree of information disclosure because of too rigid or complex security policies then they choose an extreme attitude: "When it comes to sharing, users often share too much or nothing at all" (Toninelli et al., 2009). As mentioned before the term *improper access* can be connected with the need and wish of users to gain control over the amount and granularity of location information given away, depending on the relationship and other social factors.

Tsai et al. (2010) show in their survey that participants are very concerned about who has access to their location data and that they have no control over it. The concerns, participants mentioned, were that anyone could know where one is, find him and therefore no privacy is given any more. Users' location history could be used for stalking or criminals could find out if there is nobody at home. People simply don't like it, if others whom they want to avoid can find them. Other possible harms are to be found when somebody wants to be alone, being tracked by the government and receive ads that adapt based on users location. People seem to less care about being judged about their real location and the activities they are participating.

At the end of the survey more participants became more concerned about who is getting their location data. Participants that have children see more benefits of LBS. In general the perceived benefits are finding someone in emergency or tracking children. Nevertheless the risks outweigh the benefits and users find LBS not useful.

They mention that the applications available on the market don't address users concerns of having control over ones location data. There are not enough rules or possibilities for users to adjust the settings, or if possible, it is not easy to do that. Also they state that despite the possibility to turn off location identification, users simply leave it on, because it is easier to do so.

Barkhuus et al. (2008) follow a somehow different approach. They have developed the tool Connesto that was installed on mobile phones of two groups of participants. The application allows tagging and sharing automatically ones location to a group of people. Beside other effects the authors also observed if there are any concerns regarding privacy. The result was that participants showed little concerns about privacy. One reason is the manual setting of hiding ones position. This feature helped to ease participants using such an application, although they didn't use it. They further mention that this is also an effect of a broader use of mobile phones in Europe and Japan in comparison to the US, where the most privacy related literature comes from.

Perusco and Michael (2007) describe legal and ethical, social and technological issues regarding LSB and they look at this topic from a rather psychological perspective. LBS offer many helpful solutions, which on the other side can have negative impacts that cannot be identified on first sight. An advantage for one person can be a big disadvantage for another, like in tracking and monitoring services. LBS can be used to monitor ill or disabled people and help them in different ways. Monitoring that way, is liberating for family members, but cuts the autonomy of the ones who are monitored, which can cause a feeling of desperation and helplessness, which further can cause resistance and can be counterproductive. For a good working relationship trust is essential. But monitoring somebody and intrusion into his privacy can lead to loss of trust. From a social perspective also Anthony et al. (2007) look at the privacy preferences of users according to place and find that privacy preferences/concerns vary across place and context. They found that users are more wiling to share information with others if they are alone and less if they are already together in a group or in public places. When they are alone they are less concerned about privacy, because location questions can be seen as a question or invitation to do something together. In the second case they feel that they are part of a group and not interested in further communication.

4.4 Errors

This dimension deals with errors, which can be of deliberate or accidental nature, in personal data or, in our context, with location data. Most privacy concerns are related to accidental errors in data (Smith et al., 1996). In the context of LBS this could mean that location data is erronously stored in the first place or becomes erronous by false data handling. False data could have negative impacts on the users of LBS application, because e.g. false assumption about the usage of a LBS could be derived when relying on location data that is corrupted. This could lead to privacy concerns from a user perspective.

During our research, based on the research methodology we defined at the beginning, we found very profound material that deals with at least one of the three former discussed dimensions. Interestingly not much of the work that we found tackles errors of personal or location data in depth. In the context of this work, that could mean that this dimension of privacy concern does not or only little adapt to LBS or that not much of scientific research has been conducted. We found one empirical study by Junglas and Spitzmüller (2006), which uses taxonomies and connects personality traits to the privacy concern dimensions by Smith et al. (1996). The dimension *errors* is utilized in this study, but not thoroughly explained or investigated. No statements are made regarding the types of errors that people are concerned about.

Another work we found is by Perusco and Michael (2007) and it deals to some extent with technological issues regarding LBS. They state that with ongoing developments in LBS and data processing, the whole flow of data, between a users' device and a system in the background, has becomes more efficient. Users need to have reliable LBS solutions, especially if they use such a technology on a daily basis. It is even more important, if LBS is used for e.g. monitoring of ill and handicapped people. People could see LBS as a restriction in their daily life and this could lead to wrong operation of devices. Perusco and Michael state that technological issues should not be underestimated, then "when technology fails, it creates a potential dangerous situation" (Perusco & Michael, 2007). No technology is fail-safe and as with other technologies, users have to be prepared for the consequences if LBS fail. If the technology is not failsafe then errors in such LBS can also be the result. The technology is important when coping with errors, but this work doesn't go into detail how users perceive such errors. Therefore these two mentioned papers can only be understood as describing the error dimension in a rather abstract way. They just give some hints that this dimension could pose a privacy risk for users.

5. Conclusions

With ever more mobile devices the use of LBS is also increasing. This technology bears a lot of benefits to users but also threats. One of the most important threats is the privacy that is at stake when using such services that work with location information. In this work we conducted a literature review that analyzed the scientific work along four dimensions: 1) collection, 2) unauthorized secondary use, 3) improper access, 4) errors. The collection of data is of concern to some users, but not as much, because the abuse of that information is perceived to happen in later stages of the information processing. The benefits of LBS can only be exploited if data is shared, but users perceive the collection of data differently. The concerns mentioned here were the storage location of data and the duration of storage. Consequently the duration of storage implies that data is available to a third party for a longer period and can be used for not authorized actions like tracking, observation or combination with other data for further purposes. To overcome users' concerns privacy enhancing measures like third party seals or devices based

features are used by providers. If users perceive that these measures bring benefits in the long run, they are more willing to accept LBS and share data. Who gets the users location information is a great concern for many users. Users often feel unsure about the granularity and amount of data that is available for others. Even though users widely use LBS, they want to have the possibility in their hands to distinguish between individuals who get to know their location. It is much easier for people if a friend or family member is receiving the location data than e.g. the employer. Trust plays here the crucial role. People can benefit from LBS in emergency situations and many are willing to use LBS to be sure that their family members feel good and are not in danger. This can lead to a feeling of security; on the other hand individuals who are monitored can feel powerless and depressed.

In the context of LBS the dimension *errors* is apparently not so much the source of user privacy concerns. This is an interesting finding and can be seen as a gap in the current scientific literature. To find out if deliberate or accidental errors that occur in the use of LBS are of much concern to users, further research in this area should be conducted. Another interesting point is the use of LBS in social networks. User concerns can be seen from another perspective, from the social dimension. LBS could increase concerns regarding the use of social networks and a broader understanding of this social dimension could also be aim of future research.

References

Android. (2011, 12 24). *AndroidOS*. Retrieved from http://www.android.com/

Anthony, D., Kotz, D., & Henderson, T. (2007). Privacy in Location- Aware Computing Environments. *IEEE Pervasive Computing*, pp. 64-71.

Apple. (2011, 12 24). *Apple Iphone*. Retrieved from http://www.apple.com/iphone/

Barkhuus, L., & Dey, A. (2003). Location-Based Services for Mobile Telephony: a study of users' privacy concerns. *Proceedings of the INTERACT 2003, 9TH IFIP TC13 International Conference on Human-Computer Interaction.*

Barkhuus, L., Brown, B., Bell, M., Hall, M., Sherwood, S., & Chalmers, M. (2008). From Awareness to Repartee: Sharing Locating within Social Groups. *CHI 2008* (pp. 497-505). Florence: ACM.

Clarke, R. (2001). Person-location and person-tracking: technologies, risks and policy implications. *Information Technology & People, Vol. 14, Iss: 2*, pp. 206 - 231.

Gartner. (2011, 12 24). *Gartner Newsroom*. Retrieved from http://www.gartner.com/it/page.jsp?id=1764714

Jacsó, P. (2005). Google Scholar: the pros and the cons. *Online Information Review, Vol. 29, No.2*, pp. 208-214.

Junglas, I., & Spitzmüller, C. (2006). Personality Traits and Privacy Perceptions: An Empirical Study in the Context of Location-Based Services. *Proceedings of the International Conference on Mobile Business (ICMB'06)*.

Lederer, S., Mankoff, J., & Dey, A. K. (2003). Who Wants to Know What When? Privacy Preference Determinants in Ubiquitous Computing. *CHI 2003* (pp. 1-2). Ft. Lauderdale: ACM.

Minch, R. (2004). Privacy issues in location-aware mobile devices. *Proceedings of the 37th Annual Hawaii International Conference on System Sciences.*

Perusco, L., & Michael, K. (2007). Control, trust, privacy, and security: evaluating location-based services. *IEEE Technology and Society Magazine, Vol:26, Issue: 1*.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns About Organizational Practices. *MIS Quarterly, 20 (2)*, pp. 167-196.

Solove, D. J. (2006). A Taxonomy Of Privacy. *University of Pennsylvania Law Review, Vol.154, No.3*, pp. 477-560.

Times Higher Education. (2011, 12 29). *Times Higher Education - World University Rankings, education news and university jobs - Citation averages, 2000-2010, by fields and years*. Retrieved from http://www.timeshighereducation.co.uk/story.asp?storycode=415643

Toninelli, A., Montanari, R., Lassila, O., & Khushraj, D. (2009). What's on Users' Minds? Toward a Usable Smart Phone Security Model. *Pervasive Computing, IEEE, Vol. 8, Issue: 2*, pp. 32 - 39.

Tsai, J. Y., Kelley, P. G., Cranor, L. F., & Sadeh, N. (2010). *Location-Sharing Technologies: Privacy Risks and Controls.* Carnegie Mellon University, Pittsburgh.

Xu, H., & Teo, H.-H. (2004). Alleviating Consumer's Privacy Concerns in Location-Based Services: A psychological Control Perspective. *Twenty-Fifth International Conference on Information Systems*, (pp. 793-803).

Xu, H., Teo, H.-H., & Y., T. C. (2005). Predicting the adoption of location-based services: The role of trust and perceived privacy risk. *Twenty-Sixth International Conference on Information Systems*, (S. 897-907).