Towards a New Classification of Location Privacy Methods in Pervasive Computing

Mads Schaarup Andersen and Mikkel Baun Kjærgaard

Department of Computer Science
Aarhus University
{masa,mikkelbk}@cs.au.dk

Abstract. Over the last decade many methods for location privacy have been proposed, but the mapping between classes of location based services and location privacy methods is not obvious. This entails confusion for developers, lack of usage of privacy methods, and an unclear roadmap ahead for research within location privacy. This paper presents a two-dimensional classification of existing methods for location privacy grouping them by the type of location based service to which they apply and location privacy method category. The types of location based services identified are *Point-of-Interest, Social Networking, Collaborative Sensing*, and *Route Tracing*, and the high level location privacy method categories are *Anonymization, Classical Security, Spatial Obfuscation, Temporal Obfuscation*, and *Protocol*. It is found that little work exists on location privacy in the areas of Social Networking and Collaborative Sensing, and that insufficient work has been done in Route Tracing. It is concluded that none of the existing methods cover all applications of Route Tracing. It is, therefore, suggested that a new overall method should be proposed to solve the problem of location privacy in Route Tracing. Furthermore, future challenges are identified.

Keywords: Location Privacy, Pervasive Computing, Ubiquitous Computing.

1 Introduction

With the number of smart phones based on Android and iOS soon exceeding the number of stationary and laptop computers on the Internet, applications for these devices, usually referred to as Apps, are penetrating the everyday life of people. One of the interesting aspects of Apps is that they are able to incorporate sensor data from the device and use it to provide services based on this. Currently, many apps are available for these devices and a subset of these use the location of the device (computed in some way using one or more sensors) as an integrated and essential part. These are called location based services (LBSs). In February 2010, there were 6,400 LBSs in Apples AppStore and more than 1,000 LBSs in Androids Marketplace[1]. Using location as an integrated part of

[1] http://skyhookwireless.com/locationapps/

A. Puiatti et al. (Eds.): MobiQuitous 2011, LNICST 104, pp. 150–161, 2012.

an application has enabled a number of new application domains such as navigation, friend finder, route tracking, etc. However, these services require the user to disclose his location. This introduces the concern of preserving the privacy of the user. In 1993, Bellotti and Sellen recognized that ubiquitous computing is particularly prone to attack on privacy [5] and in 2001, Langheinrich proposed six guidelines to system design to include privacy concerns [26]. Since then a lot of different methods for location privacy have been introduced, but each of them for a specific application domain and usually to solve a very specific problem. This makes it difficult for a developer to choose how location privacy should be obtained, and hence location privacy methods are often not added. Furthermore, there seems to be a lack of work in location privacy for other than Point-of-Interest (POI) services, e.g., GPS navigation, where a user can query a service for route to an address. However, during recent years new types of LBSs have emerged where the usage of location has become increasingly complex. Position is no longer shared only with a service, but might also be shared with other users in real time. Furthermore, other things than just the position might be shared with the position receiver making things such as recommender services possible. This makes it interesting to categorize LBSs in relation to location privacy, and thereafter place the existing location privacy methods using this categorization.

The contribution of this paper is twofold. The first contribution is to provide an overview of how existing location privacy methods relate to different types of LBSs, hence aiding the developer in the choice of privacy method. This is done using a two-dimensional classification scheme with *type of LBS* on one axis and *high level location privacy method* on the other. The existing work is then placed in this categorization, and hence a developer can consult it to choose an appropriate method for his location enabled app. The second contribution of this paper is to provide the research community with a road-map for research in location privacy. This is done by analyzing the above mentioned overview to reveal gaps in research. It will then be considered whether the location privacy methods of the classification can solve the gaps, and if this it is the case that a category has issues that cannot be solved with existing methods, a new method will be proposed.

Several other papers have addressed the problem of surveying and classifying location privacy methods. Krumm [25] identifies a number of open research questions in location privacy by identifying location privacy methods, attacks on these, and by surveying the results of empirical studies. Scipioni and Langheinrich [34] recognize the need for further research to be done in relation to location privacy in the newer LBS category of Social Networking (SN) services, and they propose a categorization of LBSs based on the multiplicity between sender and receiver of location. Christin et. al [8] survey the entire area of privacy in participatory sensing including location privacy. However, the three mentioned papers lack a way to make the coupling between existing methods and how they can be applied to different categories of LBSs.

The rest of the paper is structured as follows. Section 2 and Section 3 describe the two dimensions of the classification. Section 4 places the existing methods in the classification. Section 5 covers open challenges and Section 6 provides a conclusion.

2 Categories of Methods for Location Privacy

In the following we present our categorization of location privacy methods. This is based one a categorization proposed by Andersen [3], which builds on the work of Duckham and Kulik [12]. In this paper we divide privacy methods into the five categories of: *Anonymity*, *Classical Security*, *Spatial Obfuscation*, *Temporal Obfuscation*, and *Protocol*. We elaborate on these categories in the following:

Anonymity methods obtain privacy by hiding the identity of the user when providing the location. It is therefore possible to see the exact location, but impossible to tie any user to the location. A sub-category of anonymity is *pseudonymity* where the user's real identity is replaced by a pseudonym, and the idea is then that it should be impossible for an adversary to use this pseudonym to identify the user's real identity.

Classical Security methods provide privacy using classical security methods. This can be either *cryptography* or *security policies*. In cryptography the position can be encrypted using either a secret or public key encryption scheme (usually public key), so that only the provider and consumer of the position will be able to read the contents, hiding it from adversaries. When using security policies it can be expressed who can and cannot gain access, similar to access control lists in file systems.

Spatial Obfuscation methods obtain privacy by obfuscation the position of the user in space. This means that rather than providing a single point as the location an area A is provided to the position receiver.

Temporal Obfuscation methods provide privacy by obfuscating the position of the user in time. This means that instead of providing the user position in real time, the location is provided at an obfuscated position in time by adding Δt.

Protocol Privacy is obtained by having a custom protocol to enhance the privacy. This is usually used in combination with anonymity or spatial obfuscation to either hide the user identity or aid in obfuscating the position.

3 Categories of Location Based Services

In this section we will provide a categorization of LBSs. The categorization is defined in relation to relevant properties of location privacy methods. This is partly inspired by Andersen [3] who proposes LBS categories and Scipioni and

Langheinrich [34] who divide SN services into categories based on multiplicity between sender and receiver. It is our claim that the latter applies to a broader range of LBSs than just SN. Besides that we include details about the position sensitivity, importance of ID, and whether the position is shared in real time. We use this to emphasize what differs between the types of LBS that we identified. The interesting properties are:

Receiver. Who is receiving the position? This can either be a *service* which is running on a server or it can be *peers* where other users will use the position. A last option would be the case where the service runs locally, as it is the case in most car navigation devices. However, if everything runs locally the privacy concerns change. If the phone is stolen it is suddenly a threat to the privacy if sensitive information is located on the phone. This is, however, not in the scope of the privacy of intended sharing of positions and is therefore omitted.

Number of Receivers. The number of users which will receive the position. Can be 1 or n.

Number of Users. The number of users which need to provide their position in order for the LBS to make sense. Can be 1 or n.

ID Importance. How important is it for the LBS to know the true identity of the user. Can be *High*, *Medium*, or *Low*. High means very important, medium means that it depends on the specific application, and low means that it is not needed.

Spatial Sensitivity. How important is it to place the user in an exact point rather than an area. Can be *High*, *Medium*, or *Low*. High means that exact position is needed, medium means that it depends on the specific application, and low means that an area can be provided instead.

Temporal Sensitivity. How important is it that the user is placed in time. Can be *High*, *Medium*, or *Low*. High means that the LBS needs the time, medium means that it depends on the specific application, and low means that time is never essential.

Sharing Phase. Is the data shared in real time, or at a later stage. Referred to as *online* (real time) and *offline* phases.

In our categorization of LBSs, we will call the simple request-reply applications *Point-of-Interest* (POI), everything concerned with social networks *Social Networking* (SN), and participatory sensing *Collaborative Sensing* (CS) as we in the CS category focus on the type of LBSs where users share data with everybody. Furthermore, none of the three mentioned categories cover an emerging type of LBS, namely *Route Tracing* (RT). In this category of LBSs, instead of sharing a single position, the user shares a trace of coherent positions. The four categories are explained in detail in the following. Table 1 lists the important properties in relation to location privacy for the four mentioned categories.

Table 1. Important location privacy properties of the four categories of LBSs

	POI	SN	CS	RT
Receiver	Service	Peers	Service	Peers or Service
# Receivers	1	n	n	n
# Users	1	1	n	1
ID Importance	High	High	Low	Medium
Spatial Sen.	High	Medium	High	Medium
Temporal Sen.	High	High	High	Medium
Sharing Ph.	Online	Online	Online or Offline	Offline

Point-of-Interest. POI services are the first LBSs which appeared. Here a user sends a request to a server for nearest POI. This can e.g. be gas stations or the local weather forecast, and the service then replies with a set of coordinates, localized information, or possibly a route direction to the POI. In POI services, a single user queries a server to find the nearest POI. I.e. we have a 1 to 1 relationship between users and receivers. As the server needs to know who to send the reply to, ID has high importance. POI services are highly spatial sensitive as the precision of the reply depends on it. When the user is moving, POI services are, furthermore, very sensitive in regards to temporal aspects. POI services are only relevant in an online phase.

Social Network Services. SN services have become popular over the last few years with the wide adaption of Facebook Places[2], Google Latitude[3] etc. In these services, users share locations (and optionally meta-data) with friends, which are considered *peers*. SN services have a 1 to n relationship between providers and consumers, as the provider wants to share his data with a well defined (sharing with all is also considered well defined) set of receivers. As SN services are in nature self-promoting, the ID of the user is very important. Spatially, the sensitivity is of medium importance, as it is only important to tie the user to a place which might be defined as an overall area, e.g., in Facebook places where the user's location might be a building complex. Temporal sensitivity is also high as it is not interesting for receivers to know that the user at some point was at a concert if the receivers are trying to meet up with the person. SN services are interesting in an online phase.

Collaborative Sensing. In CS services, the users collect data and provide them for a service and potentially all other users. An example of this is a traffic monitoring system such as the one provided by Google Maps[4]. CS services have an n to n relationship between sender and receivers as it is vital that all the users participate for the service to make sense, and that everybody can access the data. The ID of the individual user is of low importance as it is rather the

[2] `http://www.facebook.com/places`
[3] `http://www.google.com/latitude`
[4] `http://maps.google.com`

data he provides that is relevant to the service. Spatially and temporally the sensitivity is high as the exact position is needed as well as the position in time is important. CS services are interesting in both online and offline cases. This is illustrated by the traffic monitoring example. Here the data can be used to get a real time image of the traffic at a certain point, but the data can also be used for analysis of areas often prone to congestion.

Route Tracing. The above categories cover all LBSs where a position is shared in real-time, or in an *online* phase. However, if we want to share a trace of positions collected earlier, in an *offline* phase, we have another set of privacy challenges. In RT the users collect a trace of positions linked in time rather than a single position. An example is sharing exercises such as running routes in systems such as Endomondo[5] where users then can compete on the same routes and distance and analyze performance. Furthermore, RT is becoming widely adapted by insurance companies offering usage-based insurance. An example of this is Alkabox[6] where a box records the GPS position in conjunction with acceleration data and calculates insurance based on these in case of an accident. RT is a relatively new type of LBS but is very important as not only are people sharing exercise routes, but companies are starting to record data about their customers. Furthermore, it has been proposed to use RT for road pricing [11] and hence the government might be able to track citizens leading to a big brother scenario. It is therefore the opinion of the authors that the area of RT is of high importance. That RT should be a category on its own has not yet been proposed in the literature, but as it has different properties than the rest of the categories proposed, it is indicated that RT is not covered by any of the other categories.

In RT, the trace is shared with peers or a service, and the multiplicity between senders and receivers is 1 to n. ID in itself has medium importance depending on the specific application domain. In insurance it is necessary for the insurer to know the ID, but in exercise sharing it is less important to know the exact ID of the user. Here, characteristics of the user might be enough. Spatially, the precision needed is medium as the appropriate accuracy of the position depends on the application area. Temporally, the sensitivity is also medium as it is important to be able to place the individual positions in relation to each other. However, the positions might not need to be placed in time of day. RT is done in an offline phase.

4 Classification of Existing Methods

In the following section, we will classify the existing location privacy methods with respect to the two above mentioned dimensions. Thereafter, we will analyze the contents of the table focusing on empty or close to empty cells and reason about whether the gap has a logical explanation or it is an open area needing more research. The result of the classification can be found in Table 2.

[5] `http://www.endomondo.com`
[6] `http://www.alkabox.dk`

A challenge for the classification is that some methods combine several types of privacy methods. An example is CacheCloak [29] which is a combination of anonymity and temporal obfuscation. The papers where this is the case, are placed in the category where they fit the best by the authors judgment. In the case of CacheCloak this is anonymity. To discuss the result of the classification we start out with the filled cells:

Table 2. Classification of existing location privacy methods to high level location privacy methods and categories of LBSs

	Point-of-interest	Social Networking	Collaborative Sensing	Route Tracing
Anonymity	Mix Zones[6] k-anonymity[15] CacheCloak[29] CliqueCloak[14] Distributed Anonymity[18] Pseudonymity[33]		AnonySense[9] Traffic Monitoring[19] HitchHiking[35]	
Security	P3P Inspired[1] Confab[22] Dynamic Privacy Management[21] LocServ[32]	Loccacino[10]		
Spatial Ob.	LBAC[4] SpaceTwist[36] Grid-based[16] KNN[23] Source Simulation[28] Louis, Lester and Pierre[38] ILRQ[7] New Casper[30] Obfuscation[13] Path Confusion[20]	Proximity Queries[27]		Gaussian Noise [24] Spatial Rounding [24] Selective Hiding [31]
Temporal Ob.	Temporal Ob.[17]			
Protocol	MIST[2] Geographic Routing[37]			

A lot of work has been done on anonymization in POI [6,15,29,14,18,33]. An example is k-anonymity [15] where the user is indistinguishable among $k-1$ other users. Classical security in POI is also well covered [1,22,21,32]. An example is Confab [22] which is a framework providing basic security mechanisms for controlling access to data. Spatial obfuscation has also been a main area of interest in POI [4,36,16,23,28,38,7,30,13,20,27]. The New Casper [30] is an

example where the user is placed in a grid structure rather than in a single point. Though, not a lot of work has been done in temporal obfuscation, Gruteser and Grunwald [17] have made comments on how such a method should work. Finally, in POI work has been done in creating custom privacy enabling protocols [2,37]. An example is MIST [2] where the routing of the data makes it very difficult to track the origin of data.

In classical security for SN, some work has been done in the Loccacino project [10]. Here user controllable privacy has been tested, mainly with the use of access control lists. Within SN there has also been work in spatial obfuscation with proximity queries [27] where a threshold is used to obfuscate the position of the user.

Some work has been done in anonymization for CS [9,35,19]. An example of this is Hitchhiking [35] where the user's ID is hidden.

Lastly, there has been some work done on spatial obfuscation for RT [24,31]. An example of this is adding Gaussian Noise to a trace, hence rendering it impossible to distinguish the actual positions from the added noise [24].

Next, we will comment on the obvious empty cells in the table. One of the first things to notice is that close to no work has been done in temporal obfuscation for any category. With Table 1 in mind, this is explainable with the fact that all LBSs have high or medium temporal sensitivity, and hence the method is not well suited for LBSs. The next thing to notice in the table is that the POI category is well covered in all location method categories, and hence it should be easy for a developer to choose an appropriate method for any kind of application within this LBS category. Moreover, it seems that this area is well researched, as a large variety of methods have been proposed.

In relation to SN services, not that many methods have been proposed. Here the anonymization category is empty. In relation to our definition of SN services, this makes sense, as the purpose is for the user to share some information about himself. If the data was anonymized it would be impossible to tie this information to a user. The fact that there has only been done work in the categories of security and spatial obfuscation indicates that these categories fit well to SN, but protocol seems to be an unexplored area with possibilities.

In the CS category, there has only been published anonymization location privacy methods. This is due to the fact that when data is anonymized it is difficult to infer a specific user, and since these applications cover LBSs where user ID is irrelevant, this make sense. Sometimes it might, however, make sense to apply some of the other methods to further enhance the privacy of the participating user. This could e.g. be in a weather sensing application where an area rather than a point might be enough. Hence, CS also has unexplored areas.

Lastly, we see that RT only has work done in spatial obfuscation [24,31]. This works fine for some applications of RT, but for the applications mentioned earlier in Section 3 these methods have limited applicability. This is e.g. the case for usage based insurance. Snapping to a grid, as done in Spatial Rounding, might hide the fact that the user has driven in a certain high-risk area which would increase the insurance (depending on the insurance policy and resolution of the grid). In adding Gaussian noise there might be the problem that the insurance

company would charge the user for being in all positions (including the noise), and hence this has a potentially huge disadvantage for the user. Lastly, using selective hiding the user could choose to always hide a specific high-risk area in his trace.

As mentioned earlier, RT is becoming more and more used, and considering the mentioned possible applications it is very important to develop privacy methods which cover these as well. An observation is that other categories of LBSs are concerned with sharing a single position and RT is concerned with sharing an entire trace of positions. This observation suggests that it might be a good idea to do some research in an entirely new high level method for location privacy.

5 Open Challenges

As identified in this paper there are still a lot of open challenges in the area of location privacy. We see challenges in three main areas: *Location Privacy Methods*, *Software Engineering*, and *User Awareness*.

Location Privacy Methods require more exploration of protocol and temporal obfuscation for SN services; spatial and temporal obfuscation, protocol, and classical security for CS; and all areas of RT. Moreover, we suggest that emphasis is put on developing a new category for RT as RT has many features that differ from the other categories of LBSs. This is mainly due to the fact that a trace rather than a single position is shared. It is a challenge that for some domains of RT spatial rounding, adding noise, or using selective hiding are not applicable.

Software Engineering calls for further examination of how application developers can be aided in adding location privacy to applications. The categorization presented in this paper is the first step, but currently no tools or frameworks that can aid the developer in adding location privacy to LBSs exist. The ones that do exist are only concerned with very specific types of LBSs in mind. It would be interesting to examine the effects of providing application developers with such a tool or framework, and see if it has an impact of how often location privacy methods would be used.

User Awareness is problematic as users are not all that concerned about sharing their location with others. This is the case, even though research has shown the potential dangers of doing so. Futhermore, research needs to be done in how we make people aware of the possible dangers of sharing location data. It seems that a demand from users could drive the developers to care more.

6 Conclusion

In this paper we presented a two-dimensional classification of location privacy methods in relation to types of LBSs. In this classification we placed the existing privacy methods proposed by the research community. This will serve as

a reference for LBS developers wanting to add privacy support to applications. Furthermore, the classification had the purpose of pointing out open areas in location privacy research. The results were that POI is fully covered and less research should be focused on this area. However, there are open issues in the areas of SN and CS services where more privacy methods should be explored. Moreover, the classification showed that the area of RT, though important, is close to unexplored, and that the methods proposed do not cover all applications of RT, suggesting that none of the high level location privacy methods fits the specific purpose. It is concluded that a new category of location privacy methods is needed for this RT.

References

1. Ackerman, M.S.: Privacy in pervasive environments: next generation labeling protocols. Personal Ubiquitous Comput. 8, 430–439 (2004)
2. Al-Muhtadi, J., Campbell, R., Kapadia, A., Mickunas, M.D., Yi, S.: Routing through the mist: privacy preserving communication in ubiquitous computing environments. In: Proc. 22nd Int. Conference on Distributed Computing Systems, 2002, pp. 74–83 (2002)
3. Andersen, M.S.: On limitations of existing methods for location privacy. In: 3rd International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use (2011)
4. Ardagna, C.A., Cremonini, M., Damiani, E., De Capitani di Vimercati, S., Samarati, P.: Location Privacy Protection Through Obfuscation-Based Techniques. In: Barker, S., Ahn, G.-J. (eds.) Data and Applications Security 2007. LNCS, vol. 4602, pp. 47–60. Springer, Heidelberg (2007)
5. Bellotti, V., Sellen, A.: Design for privacy in ubiquitous computing environments. In: Proc. of the 3rd conf. on European Conference on Computer-Supported Cooperative Work, pp. 77–92. Kluwer Academic Publishers, Norwell (1993)
6. Beresford, A.R., Stajano, F.: Location privacy in pervasive computing. IEEE Pervasive Computing 2(1), 46–55 (2003)
7. Cheng, R., Zhang, Y., Bertino, E., Prabhakar, S.: Preserving user location privacy in mobile data management infrastructures (2006)
8. Christin, D., Reinhardt, A., Kanhere, S., Hollick, M.: A survey on privacy in mobile participatory sensing applications. Journal of Systems and Software (2011) (in Press) (accepted manuscript)
9. Cornelius, C., Kapadia, A., Kotz, D., Peebles, D., Shin, M., Triandopoulos, N.: Anonysense: privacy-aware people-centric sensing. In: Proc. of the 6th Int. Conf. on Mobile Systems, Applications, and Services, MobiSys 2008, pp. 211–224. ACM, New York (2008)
10. Cornwell, J., Fette, I., Hsieh, G., Prabaker, M., Rao, J., Tang, K., Vaniea, K., Bauer, L., Cranor, L., Hong, J., McLaren, B., Reiter, M., Sadeh, N.: User-controllable security and privacy for pervasive computing. In: Proc. of the 8th IEEE Workshop on Mobile Computing Systems and Applications (2007)
11. Coroama, V.: The Smart Tachograph – Individual Accounting of Traffic Costs and Its Implications. In: Fishkin, K.P., Schiele, B., Nixon, P., Quigley, A. (eds.) PERVASIVE 2006. LNCS, vol. 3968, pp. 135–152. Springer, Heidelberg (2006)
12. Duckham, M., Kulik, L.: In: Drummond, J. (ed.) Dynamic & mobile GIS: investigating change in space and time. CRC (2006)

13. Duckham, M., Kulik, L.: A Formal Model of Obfuscation and Negotiation for Location Privacy. In: Gellersen, H.-W., Want, R., Schmidt, A. (eds.) PERVASIVE 2005. LNCS, vol. 3468, pp. 152–170. Springer, Heidelberg (2005)
14. Gedik, B., Liu, L.: Location privacy in mobile systems: A personalized anonymization model. In: Proc. of the 25th IEEE Int. Conf on Distributed Computing Systems, pp. 620–629 (2005)
15. Gedik, B., Liu, L.: A customizable k-anonymity model for protecting location privacy. In: ICDCS, pp. 620–629 (2004)
16. Gidofalvi, G., Huang, X., Pedersen, T.B.: Privacy-preserving data mining on moving object trajectories. In: 2007 Int. Conf. on Mobile Data Management (2007)
17. Gruteser, M., Grunwald, D.: Anonymous usage of location-based services through spatial and temporal cloaking. In: Proceedings of the 1st International Conference on Mobile Systems, Applications and Services, MobiSys 2003, pp. 31–42. ACM, New York (2003)
18. Gruteser, M., Schelle, G., Jain, A., Han, R., Grunwald, D.: Privacy-aware location sensor networks. In: Proc. of the 9th Conf. on Hot Topics in Operating Systems, vol. 9 (2003)
19. Hoh, B., Gruteser, M., Xiong, H., Alrabady, A.: Enhancing security and privacy in traffic-monitoring systems. IEEE Pervasive Computing 5(4), 38–46 (2006)
20. Hoh, B., Gruteser, M.: Protecting location privacy through path confusion. In: 1st Int. Conf. on Security and Privacy for Emerging Areas in Communications Networks (2005)
21. Hong, D., Yuan, M., Shen, V.Y.: Dynamic privacy management: a plug-in service for the middleware in pervasive computing. In: Proc. of the 7th Int. Conf. on Human Computer Interaction with Mobile Devices & Services (2005)
22. Hong, J.I., Landay, J.A.: An architecture for privacy-sensitive ubiquitous computing. In: Proceedings of the 2nd International Conference on Mobile Systems, Applications, and Services, MobiSys 2004, pp. 177–189. ACM, New York (2004)
23. Khoshgozaran, A., Shahabi, C.: Blind Evaluation of Nearest Neighbor Queries Using Space Transformation to Preserve Location Privacy. In: Papadias, D., Zhang, D., Kollios, G. (eds.) SSTD 2007. LNCS, vol. 4605, pp. 239–257. Springer, Heidelberg (2007)
24. Krumm, J.: Inference Attacks on Location Tracks. In: LaMarca, A., Langheinrich, M., Truong, K.N. (eds.) Pervasive 2007. LNCS, vol. 4480, pp. 127–143. Springer, Heidelberg (2007)
25. Krumm, J.: A survey of computational location privacy. Personal Ubiquitous Comput. 13, 391–399 (2009)
26. Langheinrich, M.: Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems. In: Abowd, G.D., Brumitt, B., Shafer, S. (eds.) UbiComp 2001. LNCS, vol. 2201, pp. 273–291. Springer, Heidelberg (2001)
27. Mascetti, S., Bettini, C., Freni, D., Sean Wang, X., Jajodia, S.: Privacy-aware proximity based services. In: Proc. of the 10th Int. Conf. on Mobile Data Management: Systems, Services and Middleware (2009)
28. Mehta, K., Liu, D., Wright, M.: Location privacy in sensor networks against a global eavesdropper. In: IEEE Int. Conf. on Network Protocols (2007)
29. Meyerowitz, J., Choudhury, R.R.: Hiding stars with fireworks: location privacy through camouflage. In: Proc. of the 15th Annual Int. Conf. on Mobile Computing and Networking (2009)
30. Mokbel, M.F., Chow, C.-Y., Aref, W.G.: The new casper: query processing for location services without compromising privacy. In: Proc. of the 32nd Int. Conf. on Very Large Data Bases (2006)

31. Mun, M., Reddy, S., Shilton, K., Yau, N., Burke, J., Estrin, D., Hansen, M., Howard, E., West, R., Boda, P.: Peir, the personal environmental impact report, as a platform for participatory sensing systems research. In: Proc. of the 7th Int. Conf. on Mobile Systems, Applications, and Services
32. Myles, G., Friday, A., Davies, N.: Preserving privacy in environments with location-based applications. IEEE Pervasive Computing 2, 56–64 (2003)
33. Pfitzmann, A., Köhntopp, M.: Anonymity, Unobservability, and Pseudonymity - A Proposal for Terminology. In: Federrath, H. (ed.) Anonymity 2000. LNCS, vol. 2009, pp. 1–9. Springer, Heidelberg (2001)
34. Scipioni, M.P., Langheinrich, M.: I'm here! privacy challenges in mobile location sharing. In: 2nd Int. Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use (2010)
35. Tang, K.P., Keyani, P., Fogarty, J., Hong, J.I.: Putting people in their place: an anonymous and privacy-sensitive approach to collecting sensed data in location-based applications. In: Proc. of the SIGCHI Conf. on Human Factors in Computing Systems (2006)
36. Yiu, M.L., Jensen, C.S., Huang, X., Lu, H.: Spacetwist: Managing the trade-offs among location privacy, query performance, and query accuracy in mobile services. In: IEEE 24th Int. Conf. on Data Engineering (2008)
37. Zhi, Z., Choong, Y.K.: Anonymizing geographic ad hoc routing for preserving location privacy. In: 25th IEEE Int. Conf. on Distributed Computing Systems Workshops (2005)
38. Zhong, G., Goldberg, I., Hengartner, U.: Louis, Lester and Pierre: Three Protocols for Location Privacy. In: Borisov, N., Golle, P. (eds.) PET 2007. LNCS, vol. 4776, pp. 62–76. Springer, Heidelberg (2007)