Location Privacy in Location-Based Services: Beyond TTP-based Schemes

Agusti Solanas, Josep Domingo-Ferrer, and Antoni Martínez-Ballesté

Rovira i Virgili University
Department of Computer Engineering and Maths
UNESCO Chair in Data Privacy
Av. Països Catalans 26
E-43007 Tarragona, Catalonia, Spain
{agusti.solanas,josep.domingo,antoni.martinez}@urv.cat

Abstract. Location-Based Services (LBS) are gaining importance due to the advances in mobile networks and positioning technologies. Nevertheless, the wide deployment of LBS can jeopardise the privacy of their users, so ensuring user privacy is paramount to the success of those services. This article surveys the most relevant techniques for guaranteeing location privacy to LBS users. The rigid dichotomy between schemes which rely on Trusted Third Parties (TTP-based) and those which do not (TTP-free) is emphasised. Also, the convenience of both approaches is discussed and some ideas on the future of location privacy in these services are sketched.
Keywords: Anonymisation/pseudonymisation in LBS, Trust management in LBS.

1 Introduction

The Information Society rests on the Information and Communications Technologies (ICT). Location-Based Services (LBS) are becoming an important ICT and will be eventually available anywhere anytime. LBS provide users with highly personalised information accessible by means of a variety of mobile devices that are able to locate themselves, e.g. by using a GPS or a fixed network infrastructure with GSM [1]. Mobile devices are ubiquitous and services related to the user's current location proliferate. Examples of LBS are location-based tourist information [2], route guidance [3], emergency assistance [4], location-based advertising [5], etc.

The extensive deployment of ubiquitous technology is not without privacy drawbacks. By sending their locations, LBS users could endanger their security and privacy because, for example, an attacker could determine their location and track them. This tracking capability of attackers opens up many computer-aided crime possibilities (harassment, car theft, kidnapping, etc.). Also, if an attacker impersonates an LBS provider, the traffic patterns of LBS users could be influenced by false information, and the users' location could be compromised [6].

There are also other attacks which aim to identify users by means of the locations contained in their queries. By identifying users, attackers can link queries to real identities. In those ways, attackers can obtain detailed profiles of the users and send them undesired advertisements or even harass them. Some examples of techniques/attacks for identifying users are the restricted space identification (RSI) attack and the observation identification (OI) attack. The RSI attack consists in linking locations to identities by using queries which are submitted from a restricted space (e.g. if a user submits queries from his garage in a suburban house, it is easy to link those queries to his real identity by looking up who lives in that house, for example by means of a phonebook). Similarly the OI attack links queries to identities by observing where users are (i.e. the attacker knows the user's location because she can see him) and correlating this information with the location contained in their queries [7].

Several countries have taken legal initiative to cope with privacy problems related to electronic communications. In Europe, the European directive on Data Protection and Privacy [8] agrees on a set of measures to assure the privacy of the users of telecommunications technologies such as LBS. Similarly, the Wireless Privacy Protection Act [9] does the same in the US. Unfortunately, all these measures regulate well-established business models but they can hardly be applied to the new LBS that arise in ad-hoc networks created and dismantled on the fly.

Although there are many other relevant topics related to LBS (e.g profile anonymisation [10, 11], trajectories analysis [12, 13], privacy in location-based community services [14], etc.), in this article we concentrate on the methods to protect the location privacy of LBS users who send their location to an LBS provider.

1.1 Contribution and plan of this article

In this article, we provide a survey of the most relevant and recent schemes designed to offer location privacy to LBS users. We analyse, organise and classify them in two main groups: (i) TTP-based schemes and (ii) TTP-free schemes. Moreover, we sketch some ideas on the future of location privacy in LBS and some lines for future research.

The rest of the article is organised as follows. In Section 2 we suggest a classification of the methods for location privacy in LBS proposed in the literature. Section 3 is devoted to the analysis of TTP-based schemes and Section 4 studies TTP-free approaches. Finally, Section 5 contains a brief discussion and some suggestions for future research.

2 Classification of methods for location privacy in LBS

In the simplest form of communication between an LBS user (U) and an LBS provider (P), the former sends a simple query (Q) containing an ID, his location (L) and a request for information (I) that he wants to retrieve from P. Thus, a

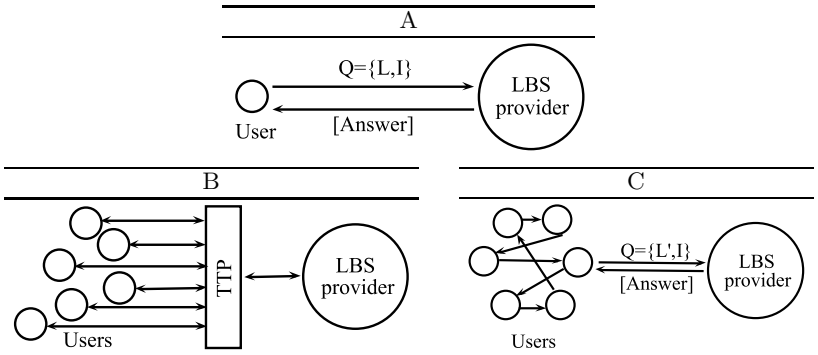

Fig. 1. A: Simple communication scheme with an LBS user and an LBS provider. **B**: Communication scheme between an LBS user, an intermediate trusted entity and an LBS provider. **C**: Communication scheme between a set of collaborative LBS users and an untrusted LBS provider. Note that in this scheme location information is not the real one (L), but a perturbed one (L') and no TTP is used.

simple query sent from U to P can be $Q = \{ID_U, L, I\} = \{ID_U, x_U, y_U,$ "Where is the closest bus station?"$\}$ (cf. Figure 1.A). By sending their current locations to P, LBS users assume that P manages their data honestly and refrains from any misuse. However, LBS providers cannot always be trusted and more complex communication schemes are needed.

Most of the solutions proposed in the literature to address the location privacy problem are based on Trusted Third Parties (TTP), i.e. entities which fully guarantee the privacy of their users. Although this approach is widely accepted, it simply moves users' trust from LBS providers to intermediate entities. By doing so, LBS providers are no longer aware of the real locations and identities of the users; trust and, by extension, power are handed over to intermediate entities such as brokers, pseudonymisers or anonymisers. The problem is that users are not necessarily satisfied by completely trusting intermediate entities or providers, especially after the recent scandals related to the disclosure of personal data by this kind of trusted entities[1] (cf. Figure 1.B).

The main difference between the simple communication scheme and the TTP-based one is that in the latter the set of intermediate entities can be expected to be smaller than the number of service providers. Therefore, intermediate entities can be well-known and the risk of trusting a dishonest entity is lessened. However, due to the above mentioned scandals, many users would prefer to trust

[1] In Autumn 2007, several data privacy disasters happened in the UK connected to Her Majesty's Revenue and Customs. Two computer disks full of personal data on 25 million British individuals disappeared; HMRC also lost another disk containing pension records of 15,000 people and a laptop containing personal data on 400 people. In 2006 in the U.S, data on 26.5 million people were stolen from the home of an employee of the Department of Veterans Affairs, and queries by 658,000 users were disclosed by the AOL search engine.

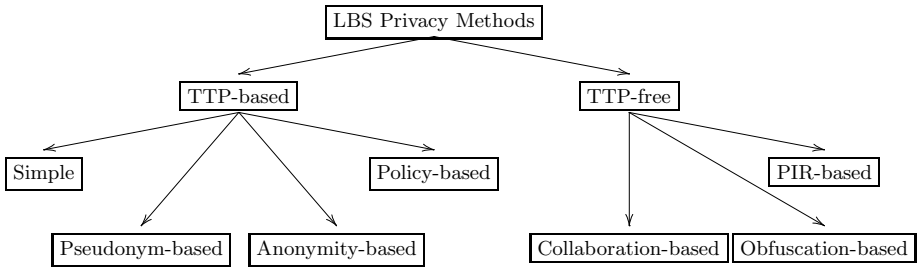

Fig. 2. Classification of location privacy methods for LBS

nobody, which leads to TTP-free schemes. These represent a substantial change of paradigm (cf. Figure 1.C). Instead of trusting a third party, users collaborate to protect their privacy. As it is explained in Section 4, there is not even need to trust the users one collaborates with. Figure 2 depicts our proposed classification of location privacy methods. The main aim of the classification is to emphasise the rigid dichotomy between these two paradigms: (i) TTP-based methods and (ii) TTP-free methods. In the following sections we review some of the most relevant representatives of TTP-based and TTP-free methods.

3 Privacy in TTP-based schemes

TTP-based schemes are very common because they are easy to understand/develop, and because, in general, they offer a reasonable trade-off between efficiency, accuracy and privacy. Moreover, some of the ideas used in these schemes arose in more mature fields like e-commerce.

In the simple scheme described in Section 2, users send their location information and queries directly to the LBS provider. In this scheme, whatever location privacy LBS users can get depends on the honest behaviour of the LBS provider.

In the following sections we concentrate on some TTP-based schemes that aim to protect the location privacy of the users.

3.1 Policy-based schemes

Policy-based schemes are one step forward in LBS privacy with respect to the simple scheme. Although the conceptual framework is the same (i.e. a user submits queries to a provider), in this case, providers adhere to a set of privacy policies known by users. Hence, if providers do not properly follow their privacy policies, users have the right to ask for a compensation and/or take legal action against providers.

Privacy policies are legal notices that contain statements defining what service providers can do with their users' personal data. Privacy policies are published by service providers, and users decide whether such policies are acceptable to them. These policies refer to many concepts and specific languages are used to define them [15, 16]. Users reach an agreement with providers about which data are collected, what are these data used for and how they can be distributed to third parties. In this kind of schemes, privacy is understood as the ability of individuals to decide when, what, and how information about them is disclosed to others. Ideally, users can choose amongst a variety of policies. So, depending on the selected policy, users can save some money but, in return, providers can distribute/sell some of their data.

These schemes are widely used on the Internet by e.g. e-commerce sites which define their privacy policies in e.g. P3P (Platform for Privacy Preferences) [17]. They have been used for automotive telematics [18], and the Geopriv (Geographic Location/Privacy) Charter of the IETF proposes their use for LBS also [19]. A recent study on the use of policies and access control techniques can be found in [20].

3.2 Pseudonymisers

Pseudonymisers are the simplest intermediate entity between LBS users and providers. Pseudonymisers receive queries from users and, prior to forwarding them to LBS providers, they replace the real IDs of the users by fake ones (i.e. pseudonyms). In this way, the real user IDs remain hidden to the provider, but pseudonymisers must store the real IDs and their corresponding pseudonyms in order to forward the answers from the providers to the users. Clearly, users must completely trust pseudonymisers, because the latter see all the location information on the former.

The main problem of this technique is that an attacker (e.g. the LBS provider herself) can infer the real identity of the user by linking the user location with e.g. a public telephone directory (e.g. by using the aforementioned RSI or OI attacks [7]).

3.3 Anonymisers

Anonymisers are the most sophisticated option in TTP-based location privacy. Instead of taking care of policies or users' identifiers, anonymisers assume that communications are anonymous, i.e. LBS providers do not require an ID to answer queries[2]. Anonymisers aim to hide users true identity with respect to emitted location information. In this section we concentrate on techniques that hide the location information of users and we assume that identifier abstraction is already guaranteed.

[2] If this assumption was not made, it would be easy to track a given LBS user by simply checking the ID or the pseudonym (like in the case of pseudonymisers).

A very common way to hide the real location of the users from the LBS provider is by using the k-anonymity property. k-Anonymity is an interesting approach to face the conflict between information loss and disclosure risk, suggested by Samarati and Sweeney [21–24]. Although it was designed for application in databases by the Statistical Disclosure Control (SDC) community, k-anonymity has been adapted to LBS privacy. In this context, we say that the location of a user is k-anonymous if it is indistinguishable from the location of another $k-1$ users. So, the fundamental idea behind k-anonymisers is to replace the real location of the user by cloaking areas in which at least k users are located. Anonymisers transform locations (x, y) at time t to $([x1, x2], [y1, y2], [t1, t2])$ where $([x1, x2], [y1, y2])$ is the rectangular area containing (x, y) between times $t1$ and $t2$ such that $t \in [t1, t2]$. By doing so, LBS providers cannot easily determine which of the k users in the cloaking area is really submitting the query.

Many examples of this kind of approach and other similar ones based on cloaking can be found in the literature [7, 25, 26]. One of the most recent advances in anonymisers is proposed in [27], where an extension of a previous anonymiser version [25] is proposed. The proposed anonymiser allows a user to define his personal privacy requirements, i.e. the number k of users amongst which he wants to be anonymised, and the maximum delay and location perturbation he is willing to accept. The proposal is resilient against identification attacks such as RSI and OI. However, it has some important drawbacks which, as we explain in the next section, can be avoided by TTP-free approaches: (i) the architecture relies on a TTP, so that the user must completely trust the platform mediating between him and the LBS provider; (ii) it is assumed that LBS providers are not malicious but semi-honest, which might turn out to be too much of an idealisation; and (iii) the architecture is centralised, which makes it vulnerable to Denial of Service (DoS) attacks.

In [28] a similar method called PrivacyGrid is described. Although the anonymiser described in [27] and the PrivacyGrid approach are very similar, the latter seems to be more efficient due to the cloaking techniques based on grids (i.e. bottom-up, top-down and hybrid) that it uses. Moreover PrivacyGrid adds the l-diversity property to the already considered k-anonymity one. By doing so, the privacy of LBS users is improved. Although PrivacyGrid seems to improve the proposal in [27], it mainly suffers from the same shortcomings.

Current research on anonymisers focuses on improving the efficiency of the intermediaries and designing highly personalised services able to guarantee the privacy of the users.

4 Privacy in TTP-free schemes

Due to the shortcomings of the TTP-based schemes, other methods that do not rely on TTPs have been proposed. First, we consider the collaboration methods that aim to obtain the same results (e.g. k-anonymity, l-diversity, efficiency) than the ones based on TTP. Then, we pay attention to the methods based on

the obfuscation of the real location without collaboration. Finally we point out a new location privacy trend based on Private Information Retrieval (PIR).

4.1 Collaboration-based methods

In [29], the first collaborative TTP-free algorithm for location privacy in LBS is proposed. The user perturbs his location by adding zero-mean Gaussian noise to it. Then the user broadcasts his perturbed location and requests neighbours to return perturbed versions of their locations. Amongst the replies received, the user selects $k-1$ neighbours such that the group formed by the locations of these neighbours and his own perturbed location spans an area A satisfying $A_{min} < A < A_{max}$, where A_{min} is a privacy parameter (the minimum required area for cloaking) and A_{max} is an accuracy parameter (the maximum area acceptable for cloaking). Finally, the user sends to the LBS the centroid of the group of k perturbed locations including his own. Since users only exchange perturbed locations, they do not need to trust each other for privacy. On the other hand, perturbations tend to cancel out each other in the centroid, so accuracy does not degrade[3]. This method does not achieve k-anonymity because the centroid is only used by a single user to identify himself. In addition, due to the noise cancellation, users cannot use this method several times without changing their location. In [30], a similar peer-to-peer scheme for location privacy is presented. Its main idea is to generate cloaking areas as in [29]: users must find other users in their cover range and share their location information. Once this information is known, users can send their queries to LBS providers using the cloaking area instead of their real locations. The main shortcoming of this proposal is that users must trust other users because they exchange their real locations. Thus, a malicious user can easily obtain and publish the location of other users. Although we classify this technique as a TTP-free technique, it can also be understood as a distributed TTP-based scheme, where each user is a TTP.

In [31], the authors propose a method based on Gaussian noise addition to compute a fake location that is shared by k users (unlike in [29]). Thus, all k users use the same fake location and the LBS provider is unable to distinguish one user from the rest, so that their location becomes k-anonymous. This method was extended to support non-centralised communications in [32]. The proposal is based on a stack of modules that progressively increase the privacy achieved by users. The basic module is equivalent to the method described in [30] where users have to trust each other because they share their location. Once they know the locations of other users, they can compute a centroid that they use as their fake location. In order to allow users to exchange their location without trusting other peers, a second module that perturbs the location is added. This module adds Gaussian noise with zero mean to the real location of users. As explained above, the centroid of locations perturbed with zero-mean Gaussian noise is quite similar to the centroid of unperturbed locations. However, if this procedure is

[3] The average of k zero-mean perturbations with variance σ^2 has zero mean and variance σ^2/k.

repeated several times with static users (i.e. users that do not change their location substantially), their real location could be deduced because of the noise cancellation (this is the main problem of [29]). To prevent this, the protocol uses privacy homomorphisms [33] to guarantee that users cannot see the real locations of other users whilst still being able to compute the centroid. Finally, a module that distributes users in a chain is added to avoid denial of service attacks to the central user. At the end of the protocol users become k-anonymous and their location privacy is secured. However, the main problem of this proposal is that it cannot provide a lower bound of the location error.

4.2 Obfuscation-based methods

Obfuscation is a TTP-free alternative to collaboration-based methods. Obfuscation can be understood as the process of degrading the quality of information about a user's location, with the aim to protect that user's privacy [34]. Some methods like the ones described in previous sections (e.g. cloaking methods) can be understood as special kinds of obfuscation because they basically modify the location information in several ways to improve user's privacy. However, we classify them in different categories because they need TTPs and/or achieve other properties such as k-anonymity or l-diversity.

In [35] an obfuscation method based on imprecision is presented. The space is modelled as a graph where vertices are locations and edges indicate adjacency. Hence, in order to obtain an imprecise location, the user sends a set of vertices instead of the single vertex in which he is located. The LBS provider cannot distinguish which of the vertices is the real one. The article proposes negotiation algorithms that allow users to increase the QoS whilst maintaining their privacy. The main problem of this technique is that users and providers must share the graph modelling the space (cf. [36] for a comprehensive approach to imprecision in location systems). Some other recently proposed obfuscation methods can be found in [37], where the real location of LBS users is replaced by circular areas of variable centre and radius.

SpaceTwist [38] is the most recent proposal for non-collaborative TTP-free location privacy. SpaceTwist generates an anchor (i.e. a fake point) that is used to retrieve information on the k nearest points of interest from the LBS provider. After successive queries to the LBS provider, SpaceTwist is able to determine the closest interest point to the real location whilst the LBS provider cannot derive the real location of the user. The main advantages of this method are: (i) no TTP and no collaboration are needed; (ii) the closest interest point is always found; (iii) the location of the user is hidden in a controlled area. However, due to the lack of collaboration, this method is not able to achieve the k-anonymity and/or the l-diversity properties.

4.3 PIR-based methods

A totally different approach to TTP-free LBS privacy is proposed in [39]. In that article, Private Information Retrieval (PIR) is used to provide LBS users

with location privacy. Although the idea of using PIR techniques is promising, the proposed approach requires the LBS provider to co-operate with users by following the PIR protocol; this prevents the use of this method in real environments, where LBS providers simply answer queries containing a location or an area without any regard for location privacy. However, if this shortcoming was solved and without significant computation and efficiency penalties, using collaborative PIR amongst peers (i.e. users) could be a really promising future research line.

5 Discussion and future work

In the above sections we have reviewed some of the most recent and relevant contributions to location privacy protection in LBS. There is a clear distinction between TTP-based schemes and the TTP-free ones. Although TTP-based schemes are the most common ones, TTP-free schemes seem superior in terms of privacy due to the following shortcomings of intermediate TTPs: (i) TTPs are critical points which can be attacked; (ii) TTPs are bottlenecks; (iii) There must be many users subscribed to a TTP for the latter to be able to compute suitable cloaking regions (offering sufficient privacy and accuracy).

In general TTP-based schemes are weak because users rely on a single trusted entity. This entity can be impersonated by a bogus TTP created by the attacker, in which case all the information shared by users with the bogus TTP falls in the hands of the attacker. A way to mount such an attack is to tamper with transmitters or use a more powerful signal.

Despite being inferior regarding privacy, TTP-based schemes are easier to implement than collaborative-based methods because all the infrastructure required by users to circumvent the use of a TTP is not necessary. However, obfuscation-based methods are also easy to implement. We believe that there is room in the market for both approaches.

The use of k-anonymity and l-diversity properties must be carefully considered because in some scenarios they are insufficient to preserve user's privacy [40]. In our opinion, there are a lot of opportunities for synergy between future work in PIR and TTP-free LBS privacy. Indeed, current PIR techniques face the (very serious) limitation of needing co-operation from the database server in following the PIR protocol. If practical PIR protocols are developed which do not need such a co-operation, it will be possible to use them for TTP-free location privacy: if a query can be submitted to a non-co-operative commercial LBS server in such a way that the latter does not learn what the query is about (i.e. the location supplied by the user), then one obtains a TTP-free LBS privacy protocol.

Acknowledgements

The authors are solely responsible for the views expressed in this article, which do not necessarily reflect the position of UNESCO nor commit that organisation. This work was partly supported by the Spanish Ministry of Education through

projects TSI2007-65406-C03-01"E-AEGIS" and CONSOLIDER INGENIO 2010 CSD2007-0004 "ARES", and by the Government of Catalonia under grant 2005 SGR 00446.

The first author thanks Dr. Paul A. Karger (IBM T. J. Watson Research Center) for his help in providing relevant references and material.

References

1. Drane, C., Macnaughtan, M., Scott, C.: Positioning GSM telephones. IEEE Communications Magazine **36**(4) (April 1998) 46 – 54 , 59
2. Simcock, T., Hillenbrand, S.P., Thomas, B.H.: Developing a location based tourist guide application. In Johnson, C., Montague, P., Steketee, C., eds.: ACSW Frontiers '03: Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003. Volume 21 of CRPIT., Darlinghurst, Australia, Australian Computer Society, Inc. (February 2003) 177–183
3. Yoo, K., Park, D., Rhee, B.: Development of a location-based dynamic route guidance system of korea highway corporation. In Satoh, K., ed.: Proceedings of the Eastern Asia Society for Transportation Studies. Volume 5., Bangkok, Eastern Asia Society for Transportation Studies (2005) 1449 – 1463
4. Reed, J.H., Krizman, K.J., Woerner, B.D., Rappaport, T.S.: An overview of the challenges and progress in meeting the E-911 requirement for location privacy. IEEE Communications Magazine **36**(4) (April 1998) 30 – 37
5. Kölmel, B., Alexakis, S.: Location based advertising. In: The First International Conference on Mobile Business, Athens, Greece (2002)
6. Karger, P.A., Frankel, Y.: Security and privacy threats to ITS. In: The Second World Congress on Intelligent Transport Systems. Volume 5., Yokohama, Japan. (November 1995) 2452 – 2458
7. Gruteser, M., Grunwald, D.: Anonymous usage of location-based services through spatial and temporal cloaking. In: Proceesings of MobiSys 2003: The First International Conference on Mobile Systems, Applications, and Services., San Francisco, CA, USA, USENIX Association, ACM, Sigmobile, ACM (May 2003) 31 – 42
8. The European Parliament and the Council: Directive 2002/58/EC on privacy and electronic communications. Official Journal of the European Communities **201** (July 2002) 37 – 47
9. 108th Congress: H.R. 71: The wireless privacy protection act. In: United States House of Representatives. (2003-4) `http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_bills&docid=f:h71ih.txt.pdf`.
10. Atluri, V., Shin, H.: Efficient security policy enforcement in a location based service environment. In Baker, S., Ahn, G., eds.: Data and Applications Security. Volume 4602 of LNCS., IFIP, Springer Berlin / Heidelberg (2007) 61–76
11. Shin, H., Atluri, V., Vaidya, J.: A profile anonymization model for privacy in a personalized location based service environment. In: 9th International Conference on Mobile Data Management. MDM'08. (2008) 73–80
12. Hoh, B., Gruteser, M.: Protecting location privacy through path confusion. In: Proceedings of the First International Conceference on Security and Privacy for Emerging Areas in Communications Networks. (2005) 194–205
13. Terrovitis, M., Mamoulis, N.: Privacy preservation in the publication of trajectories. In: 9th International Conference on Mobile Data Management. MDM'08. (2008) 65–72

14. Ruppel, P., Treu, G., Küpper, A., Linnhoff-Popien, C.: Anonymous user tracking for location-based community services. In Hazas, M., Krumm, J., Strang, T., eds.: Second International Workshop on Location- and Context-Awareness. Volume 3987 of LNCS., Springer Berlin / Heidelberg (2006) 116 – 133
15. Snekkenes, E.: Concepts for personal location privacy policies. In: ACM Conference on Electronic Commerce. (2001) 48–57
16. Cranor, L.F.: P3P: Making privacy policies more useful. IEEE Security & Privacy **1**(6) (2003) 50–55
17. W3C: Platform for privacy preferences (P3P) project. Webpage (October 2007) `http://www.w3.org/P3P/`.
18. Duri, S., Gruteser, M., Liu, X., Moskowitz, P., Perez, R., Singh, M., Tang, J.M.: Framework for security and privacy in automotive telematics. In: Proceedings of the 2nd international workshop on Mobile commerce, ACM Press New York, NY, USA (2002) 25 – 32
19. Schulzrinne, H., Tschofenig, H., Morris, J., Cuellar, J., Polk, J.: Geolocation policy. Technical report, Internet Engineering Task Force (June 2008) `http://www.ietf.org/internet-drafts/draft-ietf-geopriv-policy-17.txt`.
20. Bauer, L., Cranor, L.F., Reeder, R.W., Reiter, M.K., Vaniea, K.: A user study of policy creation in a flexible access-control system. In Czerwinski, M., Lund, A.M., Tan, D.S., eds.: Proceedings of the 2008 Conference on Human Factors in Computing Systems, ACM (2008) 543–552
21. Samarati, P.: Protecting respondents' identities in microdata release. IEEE Transactions on Knowledge and Data Engineering **13**(6) (2001) 1010–1027
22. Samarati, P., Sweeney, L.: Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression. Technical report, SRI International (1998)
23. Sweeney, L.: Achieving k-anonymity privacy protection using generalization and suppression. International Journal of Uncertainty, Fuzziness and Knowledge Based Systems **10**(5) (2002) 571–588
24. Sweeney, L.: k-anonimity: A model for protecting privacy. International Journal of Uncertainty, Fuzziness and Knowledge Based Systems **10**(5) (2002) 557–570
25. Gedik, B., Liu, L.: A customizable k-anonymity model for protecting location privacy. In: Proceedings of the IEEE International conference on Distributed Computing Systems (ICDS'05). (2005) 620 – 629
26. Cheng, R., Zhang, Y., Bertino, E., Prabhakar, S.: Preserving user location privacy in mobile data management infrastructures. In: 6th Workshop on Privacy Enhancing Technologies (PET). Volume 4258 of Lecture Notes in Computer Science., Springer Berlin / Heidelberg (2006) 393 – 412
27. Gedik, B., Liu, L.: Protecting location privacy with personalized k-anonymity: Architecture and algorithms. IEEE Transactions on Mobile Computing **7**(1) (January 2008) 1 – 18
28. Bamba, B., Liu, L., Pesti, P., Wang, T.: Supporting anonymous location queries in mobile environments with privacygrid. In: International World Wide Web Conference WWW. (2008) 237–246
29. Domingo-Ferrer, J.: Microaggregation for database and location privacy. In Etzion, O., Kuflik, T., Motro, A., eds.: Next Generation Information Technologies and Systems-NGITS. Volume 4032 of LNCS., Springer Berlin / Heidelberg (2006) 106–116
30. Chow, C., Mokbel, M.F., Liu, X.: A peer-to-peer spatial cloaking algorithm for anonymous location-based services. In: GIS '06: Proceedings of the 14th annual

ACM international symposium on Advances in geographic information systems, Arlington, Virginia, USA, ACM (November 2006) 171–178
31. Solanas, A., Martínez-Ballesté, A.: Privacy protection in location-based services through a public-key privacy homomorphism. In: Fourth European PKI Workshop: theory and practice. Lecture Notes in Computer Science, Springer Berlin / Heidelberg (2007) 362 – 368 Palma de Mallorca, Spain.
32. Solanas, A., Martínez-Ballesté, A.: A TTP-free protocol for location privacy in location-based services. Computer Communications **31**(6) (April 2008) 1181–1191
33. Okamoto, T., Uchiyama, S.: A new public-key cryptosystem as secure as factoring. In: Advances in Cryptology EUROCRYPT'98. Volume 1403 of Lecture Notes in Computer Science., Springer Berlin / Heidelberg (1998) 308
34. Duckham, M., Kulit, L.: Location Privacy and Location-Aware Computing. Number 3. In: Dynamic and Mobile GIS: Investigating Changes in Space and Time. CRC Press (2007) 35–52
35. Duckham, M., Kulit, L.: A formal model of obfuscation and negotiation for location privacy. In: Pervasive Computing. Volume 3468 of LNCS., Springer Berlin / Heidelberg (2005) 152–170
36. Duckham, M., Mason, K., Stell, J., Worboys, M.: A formal approach to imperfection in geographic information. Computers, Environment and Urban Systems **25**(1) (2001) 89–103
37. Ardagna, C.A., Cremonini, M., Damiani, E., S. De Capitani di Vimercati, Samarati, P.: Location privacy protection through obfuscation-based techniques. In Baker, S., Ahn, G., eds.: Data and Applications Security. Volume 4602 of LNCS., IFIP (2007) 47 – 60
38. 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 International Conference on Data Engineering ICDE'08. (2008) 366–375
39. Ghinita, G., Kalnis, P., Khoshgozaran, A., Shahabi, C., Tan, K.: Private queries in location based services: Anonymizers are not necessary. In: SIGMOD '08: Proceedings of the 2008 ACM SIGMOD international conference on Management of data, Vancouver, BC, Canada, ACM (June 2008) 121 – 132
40. Pareschi, L., Riboni, D., Bettini, C.: Protecting users' anonymity in pervasive computing environments. In: Sixth Annual IEEE International Conference on Pervasive Computing and Communication (PERCOM'08), IEEE Computer Society (2008) 11–19