Trusted Server Model for Privacy-Enhanced Location Based Services

Leonardo A. Martucci[1], Christer Andersson[1], Wim Schreurs[2]
and Simone Fischer-Hübner[1]

[1] Karlstads Universitet, Department of Computer Science
Universitetsgatan 2, 651-88 Karlstad, Sweden
{leonardo.martucci, christer.andersson, simone.fischer-huebner}@kau.se
[2] Vrije Universiteit Brussel, Department of Metajuridica
Pleinlaan 2, 1050 Brussels, Belgium
wim.schreurs@vub.ac.be

Abstract. Nowadays, Location Based Services (LBS) are mostly, if not always, based on the processing of location data by two players: the telecommunications service provider and the LBS provider. Assuming that these two players are different entities, we introduce in this paper a viable privacy-enhanced model for LBS based on the concept of a trusted server. Further, we provide technological, legal and economic arguments for this model. We show how to prevent an LBS provider from associating a user to an LBS request in an economically feasible way. We also show how it is possible to prevent, at the same time, the telecommunications service provider from directly associating a specific LBS request with an individual user.

1 Introduction

Location Based Services (LBS) are increasingly applied in our information society while new business models emerge fast. LBS can be described as a value-added service through communication networks based on users' locations. Typical examples of LBS are: tracking objects, finding other users, navigation, finding points of interest (e.g. nearest pharmacy) and rescue services (see [7] for more examples). LBS are offered either through LBS providers or directly by the Telecommunications Service Providers (TSP).

The current model for providing LBS to mobile phones typically comprises the following steps: (1) a user requests an LBS via a TSP; (2) the TSP forwards the request to the LBS provider; (3) the LBS provider requests the user's location from the TSP; (4) the TSP fetches the location and replies to the LBS provider; and, (5) the LBS provider delivers the requested service to the TSP, which forwards it to the user.

LBS can be divided into three general categories: pull LBS, where the user explicitly requests a LBS (e.g. find the nearest product or service); push LBS, where LBS are provided without the explicit request of a subscribed user (e.g.

a pollen alarm service); and peer-to-peer LBS involving users requesting geographical information about other users (e.g. find the nearest person).

In this paper, we show that processing location data for the provision of LBS can cause significant privacy threats for those who are located, while at the same time provoking significant security and liability implications for the involved LBS providers. We present a privacy-enhanced model for LBS, based on the idea that the TSP acts as a trusted server, including protocols for subscription, pull, push, and peer-to-peer scenarios. A short description of how billing and accountability can be performed within our model is also included. Finally, we explain how the right to privacy and user confidence in LBS can be increased by using our model, while at the same time significantly decreasing security and liability obligations for LBS providers.

The paper is organized as follows. In Section 2, we appraise the privacy and liability implications of the current LBS model. In Section 3, we survey the available LBS infrastructure and give examples of related work, while in Section 4 we describe our privacy-enhanced model for LBS and compare it with related work. Thereafter, Section 5 evaluates our model, while conclusions and final remarks are presented in Section 6.

2 Current Legal and Financial Implications

This section reviews what legal and financial implications current state-of-the-art LBS bear on the users and providers of such services.

2.1 Users' Privacy Implications

Since LBS providers process geographical information about objects and subjects, regardless whether these location data are stored or not, LBS can put a serious threat to users' privacy. Location data are usually personal data that can be related to an identified or identifiable individual, and could therefore be misused for criminal purposes, unsolicited profiling, or for revealing information about the users' social contacts. Even when consent has been given and the location data are processed accordingly, users practically lose control over what happens with their location data, what they are used for, where and how long they are stored, who has access to the data, whether they are linked with other information, and so on. Moreover, when privacy or data protection infringements take place, the user is often not even aware of these infringements. These situations can cause a significant lack of confidence on the users' side.

2.2 Implications for the LBS provider

Due to liability aspects and the rules of privacy and data protection laws, LBS providers have an interest in avoiding processing location data that can be linked to an identifiable person. If personally identifiable location data nevertheless are processed, the LBS provider needs to comply with the regulatory obligations of EC Privacy and Electronic Communications Directive 2002/58/EC [3], EC Data Protection Directive 1995/46/EC [2], and EC Data Retention Directive 2006/24/EC [4].

Art.9 I of Directive 2002/58/EC states that location data may only be processed when they are made anonymous, or with the informed consent of the users or subscribers to the extent and for the duration necessary for the provision of the LBS; users or subscribers must at any time have the right to withdraw their consent and the processing must always be restricted to what is necessary for the purposes of providing the LBS.

A requirement for anonymous LBS can also be derived from the necessity/ proportionality principle stated in Art.6 of Data Protection Directive 95/46/EC, stating that personal data must be: "adequate, relevant and not excessive in relation to the purposes for which they are collected"; and "kept in form which permits identification of data subjects for no longer than necessary for the purposes for which the data were collected" [2].

Although Art.26 of Directive 95/46/EC foresees exceptions, the transfer of personal data intended for processing to a 3^{rd} country *outside* the EU is principally prohibited according to Art.25 if that country does not ensure an adequate level of data protection. So, if the LBS provider is situated in a 3^{rd} country it cannot provide LBS from that country unless the conditions of Art.26 have been fulfilled. In addition, both directives impose very important information, security and confidentiality obligations on the LBS provider and the TSP that process data relating to identifiable persons; the impact is one of increasing financial costs and risks of liability.

Directive 2006/24/EC harmonizes the member states' provisions on the obligations for LBS providers and TSPs to retain traffic and location data for the purpose of investigation, detection, and prosecution of serious crime. Such data must be retained for not less than six months and not more than two years from the date of communication. The Directive emphasizes that "data should be retained in such a way as to avoid their being retained more than once".

Article 29 Data Protection Working Party underlines in an opinion on the use of location data for value-added services that "a high degree of protection in the processing of personal location data could be achieved if operators were to centralize requests to use a value-added service based on location data (...) and transferring the requests to the third parties responsible for providing the service in such a way that the service provider cannot identify the customer (...). Under this arrangement, the service provider can deliver the service via the operator without being able to identify the person requesting the service" [1].

3 Background

In this section, we describe the four currently most commonly proposed infrastructures for deploying LBS [12], and, further, give a few examples of existing approaches adhering to these infrastructures. We mainly consider proposals that either enable anonymity or pseudonymity:

– Anonymity is often defined as ".. the state of being not identifiable within a set of subjects, the anonymity set" [13]. The anonymity set includes all possible subjects in a given scenario, for example all possible senders of an LBS request. In the context of LBS, anonymity could be interpreted as follows: if a number of users can issue LBS requests or can be located, it is not possible for the LBS provider to identify which user in this group issued the request or has been located;
– Pseudonymity implies the usage of pseudonyms as identifiers [13]. Depending on the technique used, pseudonymity could imply everything from being in principle anonymous (using transaction pseudonyms) to being in practice identified (using person pseudonyms) [13]. One major difference between anonymity and pseudonymity is that when using pseudonyms, it is often possible to re-identify a user in case of, for instance, malicious behavior.

Each generic infrastructure incorporates a subset of the following entities (Figures 1 - 4): the user's mobile device (U), the TSP, the LBS provider (LBS), and the location intermediary (LI). The LBS provider is responsible for hosting one or more LBS applications. The TSP is providing the backbone for wireless communication among the entities. Most often, it is also responsible for localizing the mobile device on behalf of the LBS provider.

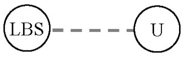

Fig. 1. Direct localization scenario.

In the infrastructure in Figure 1, a geographical positioning device is embedded in the mobile device, such as a GPS (Global Positioning System) receiver, allowing the users to control the disclosure of their location information. In an approach belonging to this category [9], so-called camouflaging techniques are proposed to blur the relationship between the users and their corresponding location by degrading the spatial and/or temporal resolution of the location information.

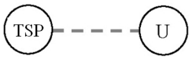

Fig. 2. Operator-portal scenario.

In the infrastructure in Figure 2, the TSP both localizes users and provides LBS. It is generally difficult to protect privacy in this type of infrastructure since the TSP knows the identities of the users "by default".

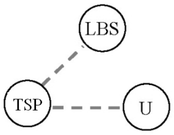

Fig. 3. Application-provider scenario.

In the infrastructure in Figure 3, LBS are offered by (3^{rd} party) LBS providers. The TSP is responsible for providing LBS providers with the users' location data. Along with the previous infrastructure, this infrastructure represents the state-of-the-art of deploying LBS. One example of a privacy-enhancing proposal belonging to this category is Mix Zones [5]: a mix zone can be defined as a spatial region where users can switch their pseudonyms in an unobservable way to prevent long-term tracking of pseudonyms.

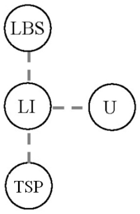

Fig. 4. Intermediary scenario.

In the infrastructure in Figure 4, a new entity, the location intermediary, is deployed between the TSP and the LBS provider to mediate requests on behalf of the user. A research prototype of an LBS architecture involving a location intermediary is currently under development within the PRIME project [8, 12]. In this proposal all involved entities communicate using an underlying anonymous overlay network. In combination with other privacy-enhanced functionalities deployed at each respective entity, this prevents the entities from colluding in order to pool their data (such as the location or the LBS request) about the users in order to create extensive user profiles.

4 Our Proposal: a Model Based on a Trusted Server

In this section we present a privacy-enhanced model, based on the idea that the TSP acts as a trusted server, for providing LBS, that prevents LBS providers from associating users with their corresponding location data.

4.1 Model Assumptions

In our model, we assume the application-provider infrastructure presented in Section 3. We describe the LBS infrastructure using four entities: users[3], TSP, LBS providers and LBS applications[4] (see Figure 5). A user is identified by his/her mobile device, and each mobile device is linked to one TSP. Multiple TSPs can request services from multiple LBS providers.

We assume a classic telecommunication infrastructure, where users are connected to the TSP through their mobile devices. In addition, we assume that mobile devices and the TSP are mutually authenticated and their communication channel is encrypted. The same assumptions are also valid for the telecommunication channel between TSP and LBS providers. Further, we assume that LBS providers know the TSP antennae geographical distribution and radio range of each antenna. This information is particular useful for providing push LBS. Finally, we assume that the mobile devices are able to perform cryptographic public key operations and generate session keys.

[3] For simplicity, we assume a one-to-one relationship between users and mobile devices.

[4] LBS applications are generally considered part of the LBS provider, but they can be modelled as an independent entity in the LBS architecture.

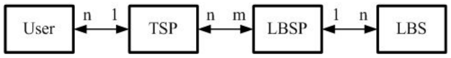

Fig. 5. Relationship between system entities.

4.2 Attacker Model

Regarding the attacker model, we assume the existence of local eavesdroppers (either monitoring the traffic between the user and the TSP, or monitoring the traffic between the TSP and the LBS provider). However, our model does not protect against an omnipresent global eavesdropper monitoring the communication between all of the entities in our model. Further, we currently do not consider to use any mechanisms to protect against *trace anonymity* (in contrast to *point anonymity* that considers the anonymity of a single LBS request); that is, the linking of a series of anonymous LBS requests to a single identity, for example by matching a number of anonymized LBS requests to a street address [10]. Finally, we assume that the TSP can detect attacks by misbehaving users that try to exhaust the resources of the TSP by, for instance, flooding the PT and RT tables (see Section 4.3) by sending pluralities of bogus LBS requests. This is because the TSP is capable of linking all incoming LBS requests to a particular user (even if the TSP does not necessarily know the content of the requests), and thus, can detect users generating multitudes of LBS requests during a short time interval.

4.3 Notation

The notation used in the rest of this paper is presented below:

- $L = \{l_1, l_2, ..., ln\}$ is the set of all LBS providers. M is a subset of L used to indicate which LBS providers a specific user is subscribing to, where $M \subseteq L$. L_{cert} is the set of certificates for all LBS providers belonging to L;
- $T = \{t_1, t_2, ..., t_n\}$ is the set of all TSP. C is a subset of cells belonging to a TSP. A cell is defined by the geographical location of the antenna and its radio range;
- $U = \{u_1, u_2, ..., u_n\}$ is the set of users;
- s represents an identifier for an LBS request, such as a LBS name, s_{req} is a LBS request message and s_{rsp} is a LBS response message[5];
- PT is the transaction pseudonym table, maintained by the TSP. Its functionality is similar to a routing table. Operations on PT are indicated between parentheses. For instance, a new entry in PT is represented using the notation $PT(newEntry)$;
- RT is the relationship table, used for providing access control services to peer-to-peer LBS applications. It stores the subset of users $V \subset U$, authorized to have access to the location information of a given user u_i, which previously subscribed to a peer-to-peer LBS application. Operations on RT are indicated in the following way: $RT_{operation}(operator)$. For instance, a new entry in RT defining the relationship between u_i and V is represented by the notation $RT_{store}(u_i \rightleftharpoons V)$.

[5] An LBS request is a packet whose source is a user and destination is an LBS provider while the LBS response has an LBS provider as source and a user as destination.

4.4 Functionality and Protocols

The LBS providers are not able to establish a relationship between users and LBS message requests in neither of the proposed scenarios. This is because the users access an LBS through the TSP. Upon receiving an LBS request from a user, the TSP removes all user-related information from the message and adds a transaction pseudonym [13] ($index_p$) to it, which is unrelated to the user, and forwards the request to the LBS provider. Therefore, from the point of view of the LBS provider, the TSP is the source of all LBS requests. In order to deliver the LBS response back to the user that requested it, the TSP maintains a transaction pseudonym table (PT).

The trust assumptions differs somewhat in the different scenarios. In all scenarios, the LBS provider is unaware of for which user it is generating a certain LBS response. This is one of the main goals with the protocol. Regarding the TSP, it will naturally know all users' locations, since it is the entity that localizes the users. Concerning the users' preferences (e.g., which services a particular user is utilizing), this information is concealed from the TSP in the case of pull services, since the LBS requests and responses are end-to-end encrypted between the users and the LBS providers. However, in the case of push and peer-to-peer services, the TSP will know the preferences of the users. This is due to the fact that the TSP is to a greater extent involved in the provisioning of the services for push and peer-to-peer services. In Section 5.3, however, we describe a possible extension which prevents the TSP from knowing the preferences of the users.

LBS Subscription Protocol: the user subscribes to a LBS provider through the TSP. Therefore, in our model, the TSP knows to which LBS providers a given user is subscribed to. In Table 1, we present the LBS provider subscription protocol for the infrastructure in Figure 5. The message msg_1 is a query for the list of available LBS providers. The TSP replies by sending the list L, along with their certificates L_{cert} in msg_2. Finally, the user sends the list of M LBS providers that he/she wants to subscribe to the TSP (msg_3).

Subscription is particularly important for push and peer-to-peer LBS applications. For push LBS applications, the user is requesting a given data set to be tracked (e.g. pollen warning service) and to be informed of events regarding this data set (e.g. increased pollen rate). For peer-to-peer LBS applications, a user has to inform the TSP which other users are allowed to have access to his/her location. Therefore, in this case the subscription protocol includes the extra message msg_4 sent from u_i to t_i, presented in Table 2. It contains an identification of the service being requested (s) and

Table 1. LBS provider subscription protocol.

msg_1	$u_i \rightarrow t_i : request\ L$
msg_2	$t_i \rightarrow u_i : L \mid L_{cert}$
msg_3	$u_i \rightarrow t_i : M$

Table 2. LBS provider subscription protocol – peer-to-peer case addition.

msg_4	$u_i \rightarrow t_i : s \mid V$
	$t_i : RT_{store}(u_i \rightleftharpoons V)$

a subset V of users allowed to have access to u_i's location data. The TSP t stores the relationship between u_i and V in its relationship table RT.

Pull LBS Protocol: when a user invokes a pull LBS application, a pull LBS request is sent to the TSP. There is no technical reason to enforce user subscription to pull LBS applications in our model, since the TSP appears to be the source of all pull LBS requests from the LBS provider's point of view. In Table 3, we present the pull LBS protocol. In msg_1, a user u_i requests access to a pull LBS application provided by the LBS provider l_a. This message includes a symmetric key K, encrypted using l_a's public key (Pb_{la}), and the service request (s_{req}) encrypted with K. If we assume that t_i demands subscription for pull LBS applications, it should verify that u_i is subscribed to l_a. If so, t_i removes all user related data from the message that could identify u_i towards the l_a, adds an $index_p$ field to the message and creates a new entry in PT. In addition, t_i adds the location data of $(x, y, z)_{u_i}$ to the LBS request and, finally, forwards it to l_a. Then, l_a decrypts the service request s_{req}, computes the service response s_{rsp}, encrypts it with K and returns msg_3 to t_i, keeping the $index_p$ field intact. After this, t_i receives the LBS message response from l_a, verifies which user is mapped to $index_p$ in PT, forwards msg_4 to u_i and removes $index_p$ from PT. Finally, the user u_i decrypts the data payload and retrieves s_{rsp}.

Push LBS Protocol: in a push LBS service, the LBS provider monitors a given set of parameters in a particular scenario. When an event happens or a threshold value is reached in a given geographical location, a message is triggered and sent to all subscribed users in, or close to, the area of interest. The push LBS protocol is described in Table 4. In msg_1, the LBS provider l_a alerts t_i that a push LBS message $PUSH_{data}$ is being generated for service s regarding a given area defined by the subset of cells C. Now, t_i retrieves the list of subscribed users inside, or close to, C. Then t_i forwards $PUSH_{data}$ to all users that are subscribing to s and are inside, or close to, C.

Table 3. Pull LBS protocol.

msg_1	$u_i \rightarrow t_i : l_a \mid E_{Pb_{l_a}}(K) \mid E_K(s_{req})$
	$t_i : u_i\_subscribed\_to\_l_a?$ *yes*: $PT(newEntry)$, *forward*
msg_2	$t_i \rightarrow l_a : index_p \mid (x, y, z)_{u_i} \mid E_{Pb_{l_a}}(K) \mid E_K(s_{req})$
msg_3	$l_a \rightarrow t_i : index_p \mid E_K(s_{rsp})$
msg_4	$t_i \rightarrow u_i : E_K(s_{rsp})$

Table 4. Push LBS protocol.

msg_1	$l_a \rightarrow t_i : s \mid PUSH_{data} \mid C$
	t_i : *verifies which users in C that are subscribed to service s*
msg_2	$t_i \rightarrow u_i : PUSH_{data}$

Peer-to-Peer LBS Protocol: a peer-to-peer LBS application demands a user to provide an explicit authorization to be localized by another user. This authorization is provided by the subscription/update protocol described in Table 2. For peer-to-peer LBS applications, the LBS provider offers geographical data only, such as maps. In Table 5 we present the protocol used by a user u_j for pinpointing another user u_i. First, in msg_1 the user u_j sends a service request s_{req} to t_i to localize u_i. Then, t_i verifies whether u_j belongs to u_i's authorized set V. If u_j belongs to V, t_i creates a new entry in PT, mapping u_j's request to $index_p$. After this, t_i assembles msg_2, which contains the service request s_{req}, the geographical position of u_i, and $index_p$. This message is then sent to l_a, which, in turn, computes the reply s_{rsp}, and sends it back to t_i (msg_3). Then, t_i receives the LBS response from l_a, verifies which user is mapped to $index_p$, and forwards s_{rsp} to u_j (msg_4). Finally, t_i removes $index_p$ from PT.

Table 5. Peer-to-peer LBS protocol.

msg_1	$u_j \rightarrow t_i : s_{req} \mid u_i$
	$t_i : u_j \in V$? *yes*: $PT(newEntry)$, *continue*; *no: stop*
msg_2	$t_i \rightarrow l_a : index_p \mid s_{req} \mid (x, y, z)_{u_i}$
msg_3	$l_a \rightarrow t_i : index_p \mid s_{rsp}$
msg_4	$t_i \rightarrow u_j : s_{rsp}$

4.5 Billing and Accountability

The main algorithm for billing could be described in the following way:

1. (a) *For pull and peer-to-peer LBS*: since each response from the LBS to the TSP relates to a specific request from a user/subscriber to the TSP (*1-1* response), the LBS provider can charge the TSP for each LBS response. Each LBS provider knows the amount of LBS responses it has generated, and, therefore, can effectively charge the TSP according to the amount of transmitted LBS responses;

(b) *For push LBS*: since a response from the LBS to the TSP does not necessarily relate to the amount of subscribers/recipients of the push service (*1-n* response), the LBS provider charges the TSP either for each response from the TSP to the user, or for each subscriber/recipient, or through a combination of both. In the last two examples, the LBS provider must get this information from the TSP[6];

2. Thereafter, since the TSP knows which users generated which requests, the TSP charges each individual user for their received LBS responses. This is possible since the TSP knows the amount of transmitted LBS responses, and the TSP can further use this information for accountability purposes in order to verify that the LBS provider is charging for a fair amount of messages;
3. Finally, the users pay the TSP, which in turn pays the LBS provider.

4.6 Comparison with Related Work

In contrast to proposals requiring extensive architectural changes, such as the introduction of location intermediaries (intermediary scenario, e.g., [8,12]) or the installation of GPS receivers in mobile phones (direct localization scenario, e.g., [9]), our proposal can be quickly deployed requiring only minor changes in the LBS infrastructure. Besides, our proposal is based on transaction pseudonyms [13], which enable users to be virtually anonymous towards LBS providers. In another proposal [6], also building on the concept of a trusted server, the authors focus their solution on the assurance of a certain level of anonymity towards the LBS users. However, in [6] no protocols are specified and no legal or economic aspects to support their proposal are presented, in contrast to our work that presents a protocol design for pull, push and peer-to-peer LBS application scenarios, supported by legal and economic aspects. The drawback with our model is, due to the fact that no additional infrastructure is used, that it defends against a weaker attacker model (see Section 4.1) than for instance [8, 12].

5 Evaluation of the Model

This section evaluates our model from a technological, legal, and economic view.

5.1 Technical, Legal and Economical Advantages

Below, we summarize the technical, legal and economical implications:

- The deployment of the proposed model is fairly simple since no extra architectural entities are demanded. Basically, the TSP has to deploy and maintain the PT and the RT tables. The LBS providers tasks are reduced, as they do not need to keep track of users. And, of course, all parties involved need to be able to handle the protocols described in this section. We argue that our proposed model is economically feasible;

[6] We assume that the TSP is trusted and does not e.g. tell the LBS provider that there is one push service subscriber, while at the same time charging many subscribers.

- If an LBS provider does not process the users' personal data, it does not need to comply with the information, security, confidentiality and availability obligations of the EU Directives. This means significant cost reductions, including: personnel, hardware, software, insurance, data storage and maintenance. This also causes much less liability risks towards LBS application users because the location data cannot be misused at the LBS provider's premises or from its servers;
- The users are not "forced" to comply with the general terms and conditions of LBS providers that can state, for instance, that the location data can be used for profiling, 3^{rd} party sharing, or data transfer to 3^{rd} countries. Concerning the TSP, there is no increase of legal obligations because the TSP always processes location data for the LBS provider, and therefore the TSP must comply anyway with the legal obligations. Although there is a measurable short-term cost of running the protocol, this cost can be shared by the TSP and LBS providers;
- From the LBS providers' point of view, the proposed billing model makes billing easier, since LBS providers do not bill individual users. Instead, they charge the TSP directly, and, for this reason, we argue that they could reduce their costs related to billing. The TSP has to charge its users individually, but this is current business practice, and, therefore, the billing workload is kept practically stable;
- Following the introduction of the EC Data Retention Directive 2006/24/EC [4], the LBS providers will risk to bear a significant part of the costs of implementing the Directive, since it does not foresee any financial compensations for the LBS providers. Our proposed model prevents the LBS providers from having access to identifiable location data, and, therefore, helps the LBS providers to save resources by avoiding the need to spend extra resources to fulfill the obligations of the Directive.

5.2 Limitations and Considerations

Below, we summarize some limitations of our approach:

- The TSP has to be trusted. Unless the TSP and the LBS providers share the $index_p$ header field of LBS messages, it is possible to guarantee, in the case of pull LBS applications, that LBS providers do not know to which specific user they are providing an LBS application, and also that the TSP does not know which LBS application is being requested by which user;
- In the case of many push and peer-to-peer LBS applications it is inevitable that a 3^{rd} party is aware of the users' service preferences. Therefore, if we want to deploy a privacy-enhanced model for LBS applications without adding new entities to the current infrastructure, either the TSP or the LBS provider should know about the users' preferences and relationship information. Nowadays, often both the TSP and LBS providers have this information (operator-portal scenario in Section 3), but in our proposed model

only the TSP has this information. The disadvantage is that the TSP possesses knowledge about both users' locations, service preferences and their relationships. However, we believe that this is the best commitment, regarding the current LBS infrastructure (application-provider scenario in Section 3), since all data is located in a single trusted entity, what makes it more easy to be protected, and, in the case of data leakage, identification of the leakage source is straightforward;

– There are also some restrictions regarding payment. An LBS provider needs to have flat rates for all pull LBS applications it offers, since the LBS provider cannot uniquely identify which users have requested which services. On the one hand, this is a restriction in the business model, while, on the other hand, it increases privacy protection as the TSP does not know which pull LBS application of an LBS provider a particular user uses. Concerning push and peer-to-peer LBS applications, there are no similar charging restrictions.

5.3 Possible Extensions

Our proposal could easily be enhanced with additional measures such as blurring the location of the requests in the same manner as in e.g. [9] (now being done by the TSP). The drawback is that it would increase the complexity of our model. Regarding push LBS, an alternative version of the protocol, more similar to the protocol for pull LBS, would be to let the users subscribe to push LBS via the TSP using relationship pseudonyms [13] (which could be changed at regular intervals). The users would still only be notified by the LSP provider (via the TSP) when a certain event occurred (for example, the user enters an area with an high incidence of pollen). The advantage in this case would be that the TSP would not know about the preferences of the the users, and, further, that billing would be easier since the LBS provider knows (through pseudonyms) how many users are subscribing to its services. However, the relationship pseudonyms would reveal more information to the LBS provider, and, moreover, the overall amount of protocol traffic would increase since more messages would be transmitted.

6 Conclusions

In this paper, we have elaborated a simple but effective privacy-enhanced method and system for LBS based on the idea of the TSP acting as a trusted server. We provided technological, legal, and economic arguments. Our model can be quickly deployed using the available infrastructure providing a win-win situation for users, TSP and LBS providers. The model prevents in the first place the LBS provider from associating a user with his/her corresponding location data. In addition, in the case of pull LBS applications, it also prevents the TSP from knowing which users request which services.

Acknowledgements

Part of this work has been sponsored by the IST FIDIS (Future of Identity in the Information Society) Network of Excellence project.

The FIDIS project receives funding from the European Community's 6th Framework Program (Contract No. 507512) and the Swiss Federal Office for Education and Science.

References

1. Art.29 Data Protection Working party. Opinion on the use of location data with a view to providing value-added services (WP 115).
2. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L No.281, 23 Nov 1995. See http://www.cdt.org/privacy/eudirective/EU_Directive_.html.
3. Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, brussels. Official Journal L No.201, 31 Jul 2002. See http://www.etsi.org/public-interest/Documents/Directives/Standardization/Data_Privacy_Directive.pdf.
4. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending directive 2002/58/ec. Official Journal L No.105, 13 Apr 2006.
5. Alastair R. Beresford and Frank J. Stajano. Location Privacy in Pervasive Computing. *IEEE Pervasive Computing*, 2(1):46–55, January 2003.
6. Claudio Bettini, X. Sean Wang, and Sushil Jajodia. Protecting Privacy Against Location-Based Personal Identification. In *Proceedings of the Secure Data Management Workshop (SDM'05)*, Sep 2005.
7. Simone Fischer-Hübner and Christer Andersson. Privacy Risks and Challenges for the Mobile Internet. In *Proceedings of the IEE Summit on Law and Computing*, 2 Nov 2004.
8. Simone Fischer-Hübner, Christer Andersson, and Thijs J. Holleboom, editors. *PRIME Public Deliverable D14.1.a - Framework V1.* 13 Jun 2005. See http://www.prime-project.eu.org/public/prime_products/deliverables/fmwk/pub_del_D14.1.a_ec_wp14.1_V4_final.pdf.
9. Marco Gruteser and Dirk Grunwald. 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)*. USENIX, 5–8 May 2003.
10. Marco Gruteser and Baik Hoh. On the Anonymity of Periodic Location Samples. In Hutter and Ullmann [11].
11. Dieter Hutter and Markus Ullmann, editors. *Proceedings of Security in Pervasive Computing: Second International Conference (SPC 2005)*. Springer Verlag, 6–8 Apr 2005.
12. Tobias Kölsch, Lothar Fritsch, Markulf Kohlweiss, and Dogan Kesdogan. Privacy for Profitable Location Based Services. In Hutter and Ullmann [11].
13. Andreas Pfitzmann and Marit Hansen. Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management - A Consolidated Proposal for Terminology v0.27, 20 Feb 2006. See http://dud.inf.tu-dresden.de/literatur/.