Ephemerality Is the New Black: A Novel Perspective on Location Data Management and Location Privacy in LBS

Mehrnaz Ataei and Christian Kray

Abstract Location information is essential to location-based services (LBS), but also has the potential to reveal sensitive information about the users of LBS to malicious agents. Therefore, location privacy is an important issue to address for both users and providers of LBS. In this paper, we investigate how location privacy can be realized in the context of a location-based service. Based on a review of architectures for LBS and key issues related to location privacy, we discuss several measures to integrate location privacy into LBS. In order to address privacy threats associated with the storage of location information, we propose an approach based on privacy-by-design principles and introduce a conceptual model to facilitate the implementation of those principles. In addition, we investigate the role of location data management in the context of privacy preservation, and propose the concept of temporal and spatial ephemerality to improve location privacy in the context of a location-based service.

Keywords Location-based services · Privacy by design · Location privacy · Ephemerality

1 Introduction

The defining feature of location-based services (LBS) is that they respond to the requests of users according to their physical location, which is not the case for other types of services. This dependency on positional information enables new and more user-friendly services but also entails issues regarding location privacy (Junglas and

M. Ataei (✉) · C. Kray
Institute for Geoinformatics (Ifgi), University of Münster, Münster, Germany
e-mail: m.ataei@uni-muenster.de

C. Kray
e-mail: c.kray@uni-muenster.de

G. Gartner and H. Huang (eds.), *Progress in Location-Based Services 2016*, Lecture Notes in Geoinformation and Cartography,
DOI 10.1007/978-3-319-47289-8_18

Watson 2008; Barkuus and Dey 2003; Fodor and Brem 2015). Striking a balance between providing a service based on the user's location while protecting their (location) privacy is thus a key challenge in this area. In principle, the location privacy of users can be compromised in two ways: (1) using real-time location information enables an attacker to find you *right now* and carry out different attacks; (2) using past data facilitates the discovery of who you are, where you live, and what you do. It can be used, for example, to predict your behavior *at any time in the future* (Krumm2009). Ideally, issues related to location privacy are considered at design time, i.e. when a location-based service is developed. The 'Privacy by Design' approach (PbD) has been applied in other domains to *"prevent privacy invasive events before they happen"* (Cavoukian 2010). It thus constitutes a good starting point for developing a process for building LBS that actively considers location privacy during the design process rather than tinkering with the service after location privacy has been compromised. The work presented in this paper proposes a new model to realize location privacy by design and an approach to tackle location privacy by focusing on the *management* of location information in LBS. We also introduce the concept of ephemerality of location data and demonstrate how it can help to address privacy threats resulting from the retention of location data. The remainder of the paper is structured as follows. We first discuss different models and architectures that have been proposed to describe the structure and inner processes of LBS. Section three reviews different approaches to location privacy. The main part of the paper (section four) outlines the basic model underpinning our approach and then reviews in detail each element and strategy for location privacy protection. The penultimate section discusses the limitations and implications of our approach. The final section summarizes our key findings and provides an outlook on future research.

2 The Anatomy of LBS

Location-based services (LBS) cover a broad range of application scenarios, from navigation support (Ran et al. 2004) over local recommender systems (Foursquare 2016) to intelligent transport services (Uber 2016) and games (O'Hara 2008). Such services are different from more conventional services as they are aware of the context in which they are being used and can adapt their contents and presentation accordingly (Steiniger et al. 2008). While a traditional service usually only relies on networking and computing resources to "collect, process, filter, transmit, and disseminate data that represents information useful for a specific purpose or individual" (Schiller and Voisard 2004), a location-based service also intrinsically considers positional information. This enables a location-based service to deliver "information to its users in a highly selective manner, by taking the user's past, present, or future location and other context information into account" (Schiller and Voisard 2004). Consequently, a location-based service is subject to additional

requirements compared to standard services (Chow and Mokbel 2009) and its architecture may also differ to accommodate those requirements. In the following, we therefore review several architectures and models that have been proposed for LBS and analyze some examples of LBS with respect to how they function.

Kido et al. (2005) proposed a location-based service model that consists of a geographic information system (GIS), a service provider and a database. In their model, a user of a location-based service obtains their location through a positioning device and then sends the position data to a service provider. The service provider, in turn, creates a response after communicating with the database and the GIS. Spiekermann (2004) developed a general communication model, which includes three layers: the positioning layer, the application layer, and the middleware layer. The positioning layer calculates the position of a user. The application layer comprises all services that request location data to integrate it into their offering. The middleware layer sits between the positioning layer and the application layer in order to reduce the complexity of service integration. All layers access the GIS directly. Strassman and Collier (2004) also discuss the development of a location-based service, a commercial friend finder application. The application is built around a location engine, which encapsulates the 'intelligence' of the service. It includes functionality such as geocoding, reverse geocoding, and routing, and retrieves data from both database and server. Deep Map (Malaka and Zipf 2000) was an early and complex location-based service providing intelligent guidance to tourists. The underlying architecture was agent-based, and components such as the routing agent or the presentation planner communicated over a shared message bus.

On a more abstract level, Hightower et al. (2002) introduced a layered approach for different positioning systems, which they termed the 'location stack'. It is inspired by similar models in the networking domain and consists of a set of layers that build upon one another. From the bottom to the top, the sensor layer deals with low-level hardware and raw data values. The measurements layer combines sensor data to derive location information such as distances or angles. The fusion layer determines the location of objects, and the arrangements layer provides information about spatial relationships between objects. The contextual fusion layer combines location information with other contextual information, e.g. to detect states. The activities layer is concerned with semantics and application-specific states, while the intentions layer deals with user needs and goals.

The example systems and the abstract architectures for LBS discussed above cover a broad range of perspectives and propose different models to conceptualize and build a service that takes into account location. One aspect that is not covered much (if at all) is the question of how location information is managed after the position of the user/device has been determined (e.g. by a set of sensors such as a GPS receiver). Few, if any of the proposed approaches consider how this information is stored and retrieved, how it can be accessed and what should happen with it 'over the long run'. This aspect is however quite central, in particular when considering privacy, which we will discuss in the following section.

3 Location Privacy

In order to receive the full benefits of a location-based service, users have to share location data, i.e. where they are or where they have been. Such location data is quite sensitive as it reveals the current physical location of users, and if disclosed would thus pose a serious threat to their privacy and safety. For example, attackers could use this information to either track them down or to exploit their absence, e.g. to break into their home while they are away. Historic location data incurs further privacy threats: attackers can, for example, use it to predict behavior (e.g. to waylay victims) or to infer information about people (e.g. where they live and work or who they know). Even though not all users are aware of these issues, the sensitivity of the location information incurs challenges and difficulties in the process of LBS adoption by users (Xu et al. 2009 and Zhou 2011).

Privacy as a concept has many facets (Waldo et al. 2008), and different definitions have been proposed—from the classic "the right to be left alone" (Warren et al. 1890) to "choose freely under what circumstances and to what extent" people share information about themselves with others (Westin 1968). Location privacy can thus be understood as privacy relating to the location information of a person, i.e. "a special type of information privacy which concerns the claim of individuals to determine for themselves when, how, and to what extent location information about them is communicated to others" (Duckham and Kulik 2006). Beresford and Stajano (2003) define location privacy along similar lines as "the ability to prevent other parties from learning one's current or past location" (Beresford and Stajano 2003).

In order to appreciate the importance of location privacy, it is important to understand the risks and threats associated with leaked location data. This is also the first step for exploring possible countermeasures to the identified threats and risks. The rapid proliferation of LBS has resulted in the collection of large amounts of location data, which, in turn, has enabled the *analysis of movement patterns*. This analysis, if applied by an attacker, is one of the most discussed threats associated with leaked location information (Krumm 2009). It has been shown that a broad range of sensitive user-related information can be extracted from analyzing movement patterns. This includes the identity of the user, their (home) address, individual (points of) interests as well as significant events (e.g. strikes or protests) that a user participated in (Hoh et al. 2006; Patterson et al. 2003).

A related issue resulting from large-scale collection of location data is *dataveillance*, "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons" (Clarke 1988). Key privacy risks associated with dataveillance (Abbas et al. 2015) are the loss of control, (continuous) monitoring, identification, social sorting, and profiling. In general, threats linked to location data have the potential to "disclose a great deal about the movements of entities, and hence about individuals associated with those

entities" (Clarke and Wigan 2011). When exploited in attacks, these threats may cause psychological, social, and economic harm (e.g. loss of control over one's life, social embarrassment, financial damage) to individuals (Clarke and Wigan 2011). Although many attacks depend on access to recorded (past) location data, the way in which location data is managed has not received a lot of attention.

In order to neutralize these and other threats to (location) privacy and to counter attacks, research has identified a number of general methods to protect privacy. One of the most common methods to secure data in general (and thus location data in particular) is encryption. Encryption is platform and service agnostic and can be applied to secure data. As a key area of cryptography, encryption provides data security through hashing and secret communication (Balogun and Zhu 2013). While cryptography is considered as an essential and necessary aspect to secure communication, it is not sufficient by itself unless its deployment and implementation are managed adequately (Kessler 2016).

In the context of location data and the associated threats, Duckham and Kulik (2006) discuss further measures for privacy protection. Regulatory strategies are a promising approach, where the government defines rules on the use of personal information, for example by passing laws that are binding for LBS providers. A second option is the use of privacy policies, which are trust-based agreements between individuals and whomever they are sharing their location data with. Another generally applicable method is to rely on anonymity. For example, a user might use a pseudonym instead of their real name or create ambiguity by grouping with other people. Finally, it is also possible to use obfuscation, which reduces the quality of location data and thereby prevents attackers from easily learning where exactly a user is located. When applied sensibly, all these methods as proposed by Duckham and Kulik (2006) can be implemented without compromising the quality of the LBS.

As a practical example of a privacy through data management implementation, Stroeken et al. (2015) developed a privacy preserving location-based service called *Zone-it,* a virtual notice board which permits users to have location-based interaction in self-zoning areas and under certain categories. The service places offers and requests with their exact coordinates on a map. Users can find offers and requests based on their interest and location (zone). After a match is found, the message disappears. Zone-it is a social media service, which shifts the focus from person-based (e.g. Facebook) to goal-oriented communication (Stroeken et al. 2015).

On a more technical level, several of the approaches listed above have successfully been implemented. Examples in this area include work by Krumm (2007, 2009), where computational countermeasures to mitigate threats are discussed including anonymity, spatial-temporal degradation, specialized queries, spatial cloaking, noise, and rounding. Other countermeasures proposed at this level are the use of a trusted third party, which improves location privacy by serving as an intermediary between providers and users of a location-based service (Mokbel et al. 2006). This intermediary can then employ various strategies, for example

dynamically adjusting location quality based on the number of nearby users. A similar approach is the use of mix zones (Beresford and Stajano 2003), which are spatial areas inside which all clients of a location-based service stop sharing their location with the service provider and also change the pseudonym they are using. This makes it difficult to track individuals when they leave a mix zone. Most of the countermeasures discussed above work based on the assumption that location data is perpetually stored. The role of location data management and its impact on location data privacy are not considered explicitly in the cited papers. Due to the increasing importance and practical relevancy of privacy, Cavoukian (2010) proposed to consider privacy from the start, i.e. the design stage. Their 'Privacy by Design' (PbD) approach describes general principles and essential steps towards realizing better privacy protection in all type of information systems. The goal of PbD is to secure the privacy of individuals by providing them with control over their information (Cavoukian 2010). For this purpose, the author defines seven basic principles that should be followed when designing an interactive system to ensure that the resulting system respects the privacy of its users:

1. **proactive not reactive**: rather than wait for privacy risks to occur, such risks should be anticipated and prevented from materializing.
2. **privacy as the default setting**: the default behavior of a system should be such that the privacy of its users are automatically protected—no prior user action is required.
3. **privacy embedded into design**: rather than 'patching' a system with some privacy-protection measures, privacy-related functionality should be considered as an integral part of the system and be realized without interfering with its overall purpose.
4. **full functionality**: unnecessary trade-offs (e.g. security vs. privacy) should be avoided and all legitimate requirements should be realized ("win-win").
5. **end-to-end security**: all data collected in the system should be protected by strong security at all stages of its life cycle (from creation to deletion).
6. **visibility and transparency**: all parties involved in the provision of a service and the running of the corresponding system, should expose their practices, policies and technologies so that they can be independently verified.
7. **respect for user privacy**: the interests, needs, and preferences of users should be considered first and foremost to ensure a user-friendly privacy-preserving system.

While the Privacy by Design approach in principle can be applied to LBS, it is not clear how it could be folded into a location-based service and how it can be used to make existing LBS more privacy-aware. In addition, the issue of managing location data is only implicitly covered and deserves a more thorough analysis due to the role historic location data plays in enabling different types of attacks. In the following section, we therefore propose a conceptual model to facilitate location Privacy by Design, and we introduce the concept of ephemerality of location data as a fundamental approach to realize Privacy by Design in the context of LBS.

4 Location Privacy by Design

Service and content providers of LBS are collecting location data from users and are usually storing it for a substantial period of time (Sathe et al. 2014). The rationale for storing the data is manifold. Depending on the country, there may be legal requirements to keep the data for at least a certain amount of time. Being able to analyze historic location data might also provide insights that can help to improve the service. Finally, historic location data also allows for deep profiling of the users, and such profiles constitute a commercial value, such as targeted advertising. From a user's perspective, in particular, the latter use can be perceived as an unwanted intrusion of their privacy.

By default, many LBS rely on a number of different databases for retaining and maintaining various types of data such as service-specific content data, digital map data, or user location data (Lee et al. 2005). These databases frequently are accessed remotely on an as-needed basis and are usually under the control of the service provider. Based on a sample of commercial LBS, the number of LBS that are self-contained on a mobile device is relatively small (e.g. navigation systems with local map databases to avoid roaming charges while traveling abroad). Research investigating how location data is stored is mostly focusing on technical challenges relating to, for example, handling large amounts of spatio-temporal location data or increasing system performance by optimizing access to location data (Mokbel et al. 2003). In the light of the various privacy threats discussed above, it makes sense to look at location data management not only from a technical perspective but also from the perspective of how it affects privacy. This aspect, however, has not received much attention in literature. When looking at existing architectures of and models for LBS such as Kivera (Schiller and Voisard 2004) or the location stack (Hightower et al. 2002), we can observe that privacy protection for location data is not an inherent part of these models. As discussed in the previous sections, there are a number of approaches to protect location privacy but these are frequently either external to the LBS, e.g. as a trusted third party (Mokbel et al. 2006), or not integrated into the architecture of a location-based service, e.g. the mix zones proposed by Beresford and Stajano (2003).

In order to describe more clearly how location privacy protection can be integrated into a location-based service, we propose a conceptual model (see Fig. 1) that facilitates applying existing methods for privacy protection as integral parts of a location-based service. In addition, the model provides means to explicitly consider how location data is managed and how strategies for privacy protection in this context can be realized. It also captures how the configuration of location privacy settings can be exposed to users of a location-based service without requiring thorough modifications of the internal core logic of a service.

The model describes how a location-based service interacts with the world and provides a user with a service while explicitly considering location privacy. A set of *sensors* observes the world and provides information about it, in particular, location data and context data. While the former refers mainly to the position of a user, the

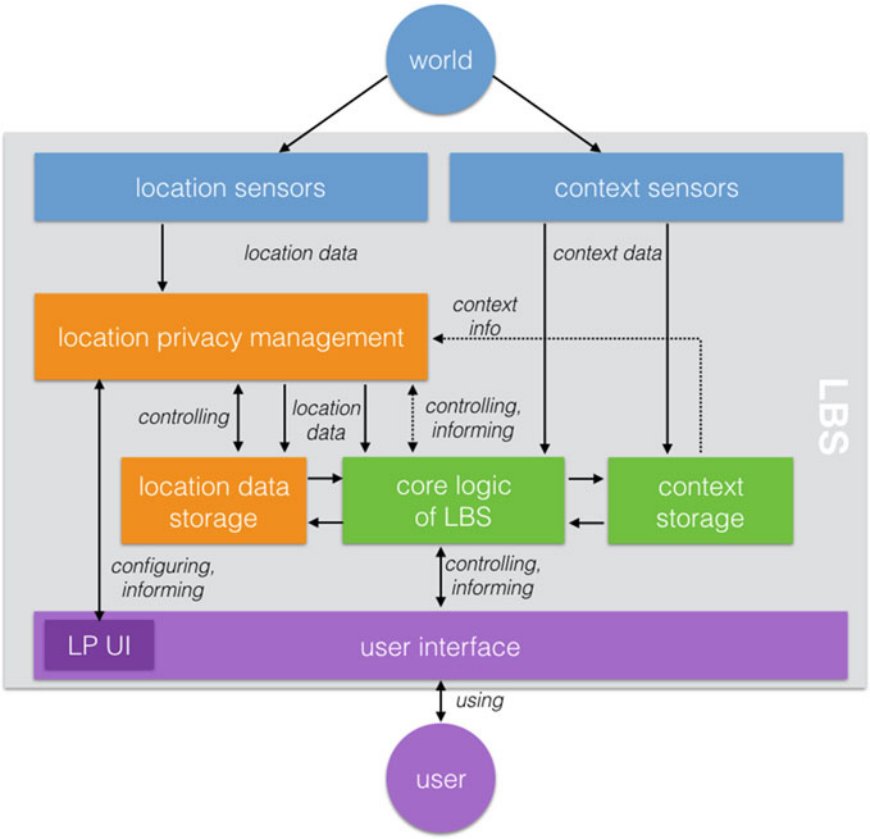

Fig. 1 A conceptual model for seamlessly integrating location privacy in a location-based service

latter includes aspects such as environmental factors, the time of the day or the current task of the user. Both types of information are usually stored for later perusal by the service (in a *location data storage* and a *context storage*). They are also needed for processing by the *core logic* of the location-based service. This part encapsulates the main functionality of the location-based service, for example, routing algorithms for a navigation service, or means to retrieve real-time traffic data. This component also interacts with both the location data storage and the context storage, i.e. to retrieve information (e.g. historic location data to carry out dead reckoning) or to update it (e.g. to set the current task of the user to navigation after directions have been requested by the user).

The *location privacy management component* (LPM) is strongly connected to the location data storage in order to implement various privacy protection measures. It observes and controls the location data storage according to the rules and procedures defined by the designers, developers and/or users of the location-based service. In order to address the location privacy issues, it can actively control the

data storage process. For example, it can reduce the quality of location data received from the sensors prior to passing it on to the location data storage or the core logic of the location-based service along the lines of the concept underpinning Caspar (Mokbel et al. 2006). From the perspective of the Core Logic, only the provider of the location data is different compared to a more traditional architecture, where it receives location data directly from the sensor component. Users of the location based service rely on a *user interface* (UI) to control the location-based service and receive information from it. The user interface can also incorporate a *location privacy user interface* (LP UI), which enables users to directly access the LPM in order to inspect how location privacy is managed and to configure it according to their preferences and needs. Providing a component which separately addresses the user interface design and options for LBS users with the goal of increasing their control over their location privacy can be a suitable approach to realize standardized privacy controls at the UI level.

The integration of the LPM and its interaction with the other components of a location-based service facilitates different ways to build a service that takes into account location privacy. In a legacy system, the LPM basically corresponds to a forwarding mechanism that forwards all location data directly to the location data storage and the core logic. A first step towards more location privacy would be to introduce a set of simple rules that the LPM uses when deciding what information to pass on to which component and at what granularity. An example of a rule is to reduce the quality of the location data to improve location privacy if the user specifies this or when the service does not require completely accurate location information to function. A more sophisticated set of rules could also take into account contextual information such as the time of the day and automatically stop providing location information after the working hours of a user are over. Such a rule set could also facilitate the realization of user-driven preferences with respect to location privacy protection (Toch et al. 2010).

The simple approach described above could be integrated into a location-based service without the need to modify the core logic (beyond changing which component provides it with location data). An alternative and complementary strategy that would also not require any changes to existing components is for the LPM to take more detailed control of the location data storage. In this case, the LPM could directly access the location data storage (e.g. using the same means that the core logic employs) to apply various strategies to recorded historic location data. For example, it could continuously monitor the stored location data to ensure k-anonymity (Sweeney 2002) (e.g. by accessing social networking sites where other people publish their location). This approach also forms the basis for the temporal ephemerality approach introduced in the following section.

More sophisticated strategies for protecting location privacy might require more involved interaction between the core logic and the LPM, and thus entail changes to the former. For example, location privacy could be negotiated on a case-by-case basis with the core logic providing a rationale why positional information of a certain quality is required. Conversely, the LPM might inform the core logic component about new location privacy settings requested by the user so that the

core logic might change its behavior in response to this. A complementary strategy is to consider the way in which location data is stored. Beyond technical considerations, there are also different options regarding how the system stores location data, where the data resides in the physical world and whom it is shared with. These aspects play a key role in the realization of spatial ephemerality as a means to protect location privacy (as discussed in Sect. 4.2).

In respect to the privacy-by-design principles, the introduction of the location privacy management component thus facilitates addressing location privacy issues from inside the LBS architecture and it supports realizing this in different ways. In addition to simplifying the integration of location privacy protection into legacy systems, the overall model of course also allows for the creation of privacy-aware LBS from scratch. The following two subsections will demonstrate the usefulness of our model further by first introducing the concepts of temporal and spatial ephemerality for location data and then highlighting how these can be realized using the LPM and the model in general.

4.1 Temporal Ephemerality

When location data is stored in LBS databases indeterminately, the window of attacks is substantially enlarged: malicious agents have an unrestricted amount of time to obtain access to the location data and carry out attacks on the user's location privacy. As discussed above, historic location data is particularly sensitive as it allows for very deep inferences on users and their behavior. In order to address this key issue of location privacy, it makes sense to consider *how long* location information is stored.

Rather than assuming that location information is stored, a more fine-grained consideration of the *temporal ephemerality* of such information can contribute towards better protecting the location privacy of the user. The basic idea of this concept is that all location information can be assigned an expiration date, after which it is deleted. By defining an expiration time and then discarding location data once it has passed, attackers will be unable to use this data for further attacks in the future (assuming that the location data storage was not breached while location data was still in the storage).

The temporal ephemerality of location data can be specified in different ways. It is possible to assign an overall expiration time for all location data, either in relative (e.g. "delete 24 h after recording") or absolute terms (e.g. "delete today at midnight"). Alternatively, a more fine-grained control is possible as well using a set of rules that determines for each individual piece of location data when it should expire. Such rules could take into account various factors such as context (e.g. "delete all location data when I leave my work place") or user preferences (e.g. "delete very precise location data immediately after recording"). The exact way in which temporal ephemerality is realized can be specified by the designer and

developers of a location-based service (while designing and building the service) and by the users while interacting with the location-based service.

In our model, the temporal ephemerality of location data can be easily realized by encapsulating the corresponding rule sets inside the LPM. For legacy LBS, this could be achieved in a completely transparent way as outlined above. The only component that would need to be modified slightly is the location data storage as each entry would get an additional attribute (expiration date) to facilitate the timely removal of expired location data. The LPM could then use this attribute to periodically query the location data storage for all entries with an expiration time in the past and to then delete the returned entries.

In addition to better protecting the location privacy of users in general, implementing temporal ephemerality of location data in this way also realizes several basic principles of the privacy-by-design approach for location data. Supporting the idea of being preventative and not remedial by discarding the data from database, the risk of inference attacks will be reduced as there will be no record of data available for attackers after the expiration date. This follows the 'proactive, not reactive' principle, where "Privacy by Design comes before-the-fact, not after" (Cavoukian 2010). With regards to the approach and implementation described above, the discarding of location data occurs automatically once the expiration time has passed, thereby realizing the 'privacy as the default setting' principle (This behavior could be changed by users, e.g. via the LP UI, should they wish to keep location data forever). Finally, the approach outlined above very strongly connects with the 'privacy embedded into design' principle of PbD. By encapsulating the functionality for temporal ephemerality in the LPM, designers can easily design systems that realize the location-based service while respecting location privacy as the other components are largely unaffected. They can focus on the location-based service functionality and relegate considerations about location privacy to LPM and (to some degree) the location data storage. The LP UI then provides an easy way to expose issues related to location privacy to users. The model also facilitates reuse of components: designers can create generic LPM, location data storage, and LP UI components and then use them to create different location privacy-aware location-based service.

4.2 Spatial Ephemerality

In the discourse of (location) privacy, many aspects are discussed but the issue of *where* location information is stored (and accessible) has received little attention. Usually, the underlying assumption is that stored location data can be accessed from anywhere. If, however, such data is only accessible inside a well-defined spatial area, then attackers or their proxies have to be co-present in order to carry out an attack. In analogy to temporal ephemerality for the time domain, the concept of *spatial ephemerality* refers to location data having a spatial 'expiration' zone: location data is stored in a particular area, and only accessible for users who reside

inside this area. More specifically, spatial ephemerality entails that all location data is assigned a spatial expiration zone, and once a user leaves the zone for a particular location entry, it is deleted. To put it differently, location data would not leave a particular geographic area (e.g. the area where the location-based service is most relevant or where the user intends to use it) so that an attacker could not use it once a user has left that area - assuming the data was not retrieved while the user was still inside the area.

Similar to the temporal case, the spatial ephemerality of location data can also be defined in relative (e.g. "delete location data that is further than 2 km from the current position") or absolute terms (e.g. "delete location data that is more than 2 km from the city center"). In addition to specifying general rules for all location data, it is possible to define this for individual pieces of location data. The rules encoding spatial ephemerality can also consider various other factors such as context (e.g. "delete all location data inside a 2 km radius around locations that are visited only by few people") or user preferences (e.g. "delete all location data inside a 2 km radius around my home"). As with the temporal case, the exact way in which spatial ephemerality is realized can be specified by the designers and developers of a location-based service (during design and development) and by the users (during usage of the location-based service).

In our model, spatial ephemerality could be realized via the LPM to encapsulate the rule set defining the spatial ephemerality of location data. This approach has the advantage of being completely transparent and thus would lend itself easily to making legacy LBS more location privacy-aware. As with the temporal case, it would be necessary to introduce an additional attribute for location data. Consequently, the location data storage component would have to be modified accordingly. This attribute would hold the spatial expiration area of an entry, for example, in the form of a polyline corresponding to the boundary of the area. The LPM could then periodically query the location data storage component with the current location to obtain all entries, which do not contain this location within their expiration areas. The returned entries could then be deleted.

Spatial ephemerality can contribute towards location data privacy by deleting location data based on spatial conditions, and thereby reduce the risk of inference attacks. The proposed model and approach to realize spatial ephemerality of location data also facilitates the application of PbD principles to location data. By geographically limiting the storage of location data and encapsulating the corresponding rules with default values inside the LPM, the 'privacy as the default setting' principle can easily be realized. Similarly, this approach supports the 'privacy embedded into the design' principle. The 'proactive not reactive' principle of PbD applies as well, as location data is systematically deleted before an attack occurs. The considerations regarding the design and development of privacy-aware LBS (ease of improving legacy LBS, concentration of location privacy concerns in the LPM, reuse of components) we discussed for temporal ephemerality (in Sect. 4.1) hold true for spatial ephemerality as well.

In order to further investigate how ephemerality can be implemented and used in everyday life, we have started to develop an initial prototype[1] based on our proposed model. The prototype is a service designed to enable users to share their experiences while visiting or exploring a city (e.g. special events). The application provides a means to share short messages anonymously with people in the same geographic area. In addition, it empowers users to define an expiration time for each message. The system design is implemented to not store any location data of the users or their messages over time. The location data of users is discarded from the system (website[2] or app) as soon as the user leaves the geographic area or when the messages expire. Our next step is to carry out user studies based on this prototype to gain a deeper understanding on how users act when they are given increased control over their location privacy.

5 Discussion

The proposed location-Privacy by Design approach and the corresponding model for LBS as well as the concept of ephemerality offer benefits and are also subject to a number of limitations. The key benefit of the PbD approach in combination with the proposed model is facilitating the realization of location-privacy-preserving LBS. In Sect. 4, we discussed in detail how this can be achieved both for existing LBS that should be made more privacy-aware and during the design of a new LBS from scratch. The benefits of the ephemerality concept include facilitating sophisticated privacy-protection without having to substantially modify all of the components of a location-based service. In addition, ephemerality of location data reduces the amount of storage needed to hold historic location data, and it provides a unified and simple approach to implement legal requirements (e.g. via expiration dates corresponding to the legally required duration of storing data). Considering that LBS can produce a large amount of privacy sensitive data every day, which requires a secure storage and proper treatment to comply with existing law, the ephemerality approach will also not require the system to obtain more servers over time, which may incur financial savings. From the user's point of view, key benefits of the proposed approach and the model as well as ephemerality include an increased level of privacy and a fine-grained control over the user's location privacy.

These benefits also come with a number of drawbacks and challenges. While there are no inherent technical issues preventing the implementation of the proposed ideas, there are potential business-related implications. Location data can have a commercial value for advertisement partners to LBS companies as the collected location data can provide deep insights into the behavior and habits of

[1] https://github.com/heinrichloewen/SC-App.

[2] https://github.com/chack05/sc16-ephemeral-lbs-server.

users. For example, providing tailored advertisements to users based on those insights can be a viable revenue stream for LBS companies, which ephemerality could negatively affect. A key question in this context is if users would be willing to pay for a service with increased privacy and control to compensate for reduced revenues of service providers due to this. With the non-permanent storage of location data also comes the challenge of maintaining the functionality of LBS that rely on forward predictions based on past behavior. Time-limited data storage could pose substantial challenges when making advance analysis of user data. Selecting expiration conditions (both spatial and temporal ones) carefully to ensure optimal service provision would be one way to address this challenge. Another limitation or drawback of the proposed LPM component is the fact that it is still vulnerable to attacks, and may also be subject to new kinds of attacks. While in principle it can reduce the severity of successful attacks aimed at retrieving historic location information (by reducing the amount of data being stored), the attacks can still be applied. In addition, the component may become a target by itself, for example, by introducing rules into the LPM component that counteract user-specified rules.

A consequence and potential drawback of using the ephemerality feature is the loss of data. This can be discussed from a provider and a user perspective. From the provider perspective, data storage allows the information they gather to be used for profiling or categorizing their users for purposes such as targeted advertising. Historical tracks of location data is a commodity that can be sold to other companies to be used for the same purposes. From the user's perspective, the loss of data can also have consequences. By not storing location information, it may not be possible to get user-adapted or a localized service provision. For applications that strongly rely on recorded location data (e.g. Foursquare), the ephemerality feature may severely affect service quality.

In section three, we have listed a number of approaches and solutions developed and proposed to protect (location) privacy in LBS. It is crucial to mention that LPM as a solution is a complementary approach. Our solution can be combined with other approaches such as encryption or anonymization. Privacy is regarded as a multifaceted problem that is challenging to solve with one single solution. Due to this, combinations of different methods and approaches can be advisable and/or necessary in order to protect the privacy of users.

In our discussion, we mainly focused on the management of location data due to its importance and potential in the context of realizing location privacy in a location-based service. We did not analyze contextual aspects in detail, which can also have a severe impact on privacy in general. One option to deal with this issue could be the introduction of a context data management component into our model that would operate on contextual data in a similar way as the LPM deals with location data. Another area we did not discuss relates to users and their understanding of location privacy. The model foresees a subcomponent of the user interface, the LP UI, as a means for users to configure settings related to location privacy and to access information about it. In order to build LBS that facilitate proper protection of the users' location privacy, these user-facing parts need to be

further investigated. In particular, there is a lack of knowledge about the user's understanding of location privacy and related concepts and options, and it is also not clear how to best communicate this to users.

6 Conclusion

In this paper, we investigated how location privacy can be realized in the context of LBS. In particular, we looked into the role of location data management in the context of privacy preservation. Based on privacy-by-design principles, we then proposed an approach tailored to LBS and defined a conceptual model to facilitate the implementation of those principles. We showed that this model supports the realization of different privacy protection mechanisms and enables an explicit and fine-grained control of location data management in the context of privacy preservation. In addition, we proposed the concept of temporal and spatial ephemerality as a means to improve location privacy in the context of a location-based service, which can both be realized using the proposed approach and model. The conceptual model and ephemerality concept are complementary to existing methods to protect location privacy such as encryption or obfuscation.

Though the proposed approach is subject to some limitations, there are several promising options for further research. One interesting and underexplored area relates to the understanding users have of location privacy, related concepts, and options, and to how to effectively communicate these aspects to them. We are planning to carry out user studies to compare different systems to communicate threats and countermeasures and to gain a deeper understanding of (mis)conceptions about location privacy. The LP UI component will serve as a platform to facilitate this line of research. A complementary direction for future research relates to the concept of spatial ephemerality. Here, we plan to investigate how opportunistic information sharing can enable spatial ephemerality at the level of the location data storage and/or the core logic of a location-based service. This line of work will rely on the LPM component to realize and to test the prototypes in realistic settings.

Acknowledgment The authors gratefully acknowledge funding from the European Union through the GEO-C project (H2020-MSCA-ITN-2014, Grant Agreement Number 642332, http://www.geo-c.eu/).

References

Abbas, R., Michael, K. and Michael, M.G., 2015. Using a Social-Ethical Framework to Evaluate Location-Based Services in an Internet of Things World. *International Review of Information Ethics*, *22*(12).

Balogun, A.M. and Zhu, S.Y., 2013. Privacy Impacts of Data Encryption on the Efficiency of Digital Forensics Technology. *arXiv preprint* arXiv:1312.3183.

Barkuus, L. & Dey, A., 2003. Location-Based Services for Mobile Telephony: a Study of Users' Privacy Concerns. In *Proceedings of the International Conference on Human-Computer Interaction (INTERACT)*. pp. 1–5.

Beresford & Stajano, F., 2003. Location privacy in pervasive computing. *IEEE Pervasive Computing*, 2(1), pp. 46–55. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1186725.

Cavoukian, A., 2010. Privac y by Design. *Identity in the Information Society*, 3(2), pp. 1–12.

Chow, C.-Y. & Mokbel, M.F., 2009. Privacy in location-based services: a system architecture perspective. *Sigspatial Special*, (2), pp. 23–27. Available at: http://dl.acm.org/citation.cfm?id=1567258.

Clarke, R., 1988. Information technology and dataveillance. Communications of the ACM, 31 (5), 498–512.

Clarke, R. and Wigan, M., 2011. You are where you've been: the privacy implications of location and tracking technologies. *Journal of Location Based Services*, *5*(3–4), pp. 138–155.

Duckham, M. and Kulik, L., 2006. Location privacy and location-aware computing. *Dynamic & mobile GIS: investigating change in space and time*, *3*, pp. 35–51.

Fodor, M. & Brem, A., 2015. Do privacy concerns matter for Millennials? Results from an empirical analysis of Location-Based Services adoption in Germany. *Computers in Human Behavior*, 53, pp. 344–353. Available at: http://www.sciencedirect.com/science/article/pii/S0747563215300066.

Foursquare. 2016. *foursquare*. [ONLINE] Available at: https://foursquare.com. [Accessed 15 June 2016].

Hightower, J., Brumitt, B. & Borriello, G., 2002. The location stack: A layered model for location in ubiquitous computing. *Proceedings—4th IEEE Workshop on Mobile Computing Systems and Applications, WMCSA 2002*, pp. 22–28.

Hoh, B. et al., 2006. Enhancing security and privacy in traffic-monitoring systems. *IEEE Pervasive Computing*, 5(4), pp. 38–46.

Junglas, I. & Watson, R., 2008. Location-based Services., 51(3), pp. 65–70. Available at: http://pewinternet.org/Reports/2013/Location.aspx.

Kessler, G.C., 2016. An Overview of Cryptography (Updated Version, 3 March 2016).

Kido, H., Yanagisawa, Y. & Satoh, T., 2005. An anonymous communication technique using dummies for location-based services. *Proceedings—International Conference on Pervasive Services, ICPS '05*, 2005, pp. 88–97.

Krumm, J., 2007. Inference Attacks on Location Tracks. *Pervasive Computing*, 10(Pervasive), pp. 127–143. Available at: http://www.springerlink.com/index/TG64551RW2716103.pdf\nhttp://research.microsoft.com/en-us/um/people/jckrumm/publications2007/inferenceattackrefined02distribute.pdf.

Krumm, J., 2009. A survey of computational location privacy. *Personal and Ubiquitous Computing*, 13(6), pp. 391–399.

Lee, D.L., Zhu, M. & Hu, H., 2005. When Location-Based Services Meet Databases. *Mobile Information Systems*, 1(2), pp. 81–90. Available at: http://iospress.metapress.com/index/d3fy03rg5vvvbc29.pdf\nhttp://www.hindawi.com/journals/misy/2005/941816/abs/.

Malaka, R. & Zipf, A., 2000. Deep Map: Challenging IT research in the framework of a tourist information system. *ENTER 2000: 7th. International Congress on Tourism and Communications Technologies in Tourism, Barcelona, Spain, 26–28 April 2000*, pp. 1–11. Available at: http://195.130.87.21:8080/dspace/handle/123456789/581.

Mokbel, M.F., Ghanem, T.M. & Aref, W.G., 2003. Spatio-Temporal Access Methods. *IEEE Data Engineering Bulletin*, 26(2), pp. 40–49. Available at: http://dl.acm.org/citation.cfm?id=1458187.

Mokbel, M.F., Chow, C.-Y. & Aref, W., 2006. The new Casper: query processing for location services without compromising privacy. *Vldb'06*, (1), pp. 763–774. Available at: http://dl.acm.org/citation.cfm?id=1164193.

O'Hara, K., 2008. Understanding geocaching practices and motivations. *Proceedings of the SIGCHI Conference on Human …*, p. 1177. Available at: http://portal.acm.org/citation.cfm?doid=1357054.1357239\nhttp://dl.acm.org/citation.cfm?id=1357239.

Patterson, D.J. et al., 2003. Inferring High-Level Behavior from Low-Level Sensors. *UbiComp 2003 Ubiquitous Computing*, 2864, pp. 73–89. Available at: http://www.springerlink.com/index/k3x004g773qj80kg.pdf.

Ran, L., Helal, S. & Moore, S., 2004. Drishti: An integrated indoor/outdoor blind navigation system and service. *Proceedings - Second IEEE Annual Conference on Pervasive Computing and Communications, PerCom*, pp. 23–30.

Sathe, S. et al., 2014. Enabling Location-Based Services 2.0: Challenges and Opportunities. *Mobile Data Management (MDM), 2014 IEEE 15th International Conference on IS–SN -*, 1, pp. 317–320.

Schiller, J. & Voisard, A., 2004. *Location-based Services*, Morgan Kaufmann.

Spiekermann, S. 2004. General Aspects of Location-Based Services. In: Schiller, J. & Voisard, A., 2004. Location-based Services. Morgan Kaufmann, pp.15–33

Steiniger, S., Neun, M., Edwardes, A. and Lenz, B., 2008. Foundations of LBS. *CartouCHe-Cartography for Swiss Higher Education. Obtido em*, *20*, p. 2010.

Strassman, M. and Collier, C. 2004. Case Study: Development of the Find Friend. In: Schiller, J. & Voisard, A., 2004. Location-based Services. Morgan Kaufmann, pp.34–48.

Stroeken, K., Verdoolaege, A., Versichele, M., Backere, F.D., Devos, D., Verstichel, S. and Weghe, N.V.D. 2015. Zone-it before IT zones you: A location-based digital notice board to build community while preserving privacy. *Journal of Location Based Services*, 9(1), pp. 16–32.

Sweeney, L., 2002. k-ANONYMITY: A MODEL FOR PROTECTING PRIVACY. *International Journal on Uncertainty*, 10(5), pp. 557–570.

Toch, E. et al., 2010. Empirical models of privacy in location sharing. *Proceedings of the 12th ACM international conference on Ubiquitous computing—Ubicomp '10*, (April 2016), p. 129. Available at: http://portal.acm.org/citation.cfm?doid=1864349.1864364.

Uber. 2016. https://www.uber.com. [ONLINE] Available at: https://uber.com. [Accessed 15 June 2016].

Waldo, J. et al. (2008), Engaging Privacy and Information Technology in a Digital Age. National Academies Press.

Warren, Samuel D., and Louis D. Brandeis. "The right to privacy." Harvard law review (1890): 193–220.

Westin, A.F., 1968. Privacy and Freedom. *American Sociological Review*, 33(1), p. 173.

Xu, H. & Gupta, S., 2009. The effects of privacy concerns and personal innovativeness on potential and experienced customers' adoption of location-based services. *Electronic Markets*, 19(2–3), pp. 137–149.

Zhou, T., 2011. The impact of privacy concern on user adoption of location-based services. *Industrial Management & Data Systems*, 111(2), pp. 212–226.