Privacy in Location-Based Services: Present Facts and Future Paths

Zakaria Sahnoune(✉) and Esma Aïmeur

Department of Computer Science and Operations Research, University of Montreal, Montreal, Canada
{sahnounz,aimeur}@iro.umontreal.ca

Abstract. The usage of Location-Based Services (LBSs) ranges from searching points of interests to location-based social networking. They are present in almost every daily task. Moreover, with smartphone ownership growth, getting one's location became easier, and the privacy-related issues became almost inescapable. Accordingly, numerous efforts have extensively explored the problem from different perspectives. Many of the existing solutions lack rigorous privacy safeguards and have been foiled by several location attacks. In a nutshell, their shortcomings are mainly due to the heavy dependence on computational privacy models, and the lack of consideration for adaptable protections. We discuss in this paper the current location-based services models, privacy issues, a general overview of the protection mechanisms, and our thoughts about location-privacy in the near future.

Keywords: Location-based services · Location Privacy Preserving Mechanisms · Privacy models · Collaborative mechanisms

1 Introduction

A Location-Based Service (LBS) is tracking your location, well one may think that it is not that bad. They may also think that they can check out the visited locations, manage them, and probably turn off location tracking entirely. While being true in some cases, an investigation done by Associated Press affirms that Google keeps gathering its users' location data even when they switch the tracking feature off [13]. In a nutshell, Google offers "apparently" an option to turn off location tracking from the account settings portal. However, even when the user disables any tracking, Google keeps collecting location-related data. One may also think that it is an individual act that cannot be generalized. Similar incidents occurred, and they keep occurring. Facebook [15], Yahoo [18], eBay [16] and others all reported serious privacy-related incident in the last 5 years. The bottom line is that such incidents are kept hidden until being forced to be revealed.

J. Li et al. (Eds.): SPNCE 2019, LNICST 284, pp. 141–151, 2019.
https://doi.org/10.1007/978-3-030-21373-2_13

To be more precise, LBSs are the application services relying on gathering and processing location data. Their primary purpose is to determine coordinates of objects such as parcels, vehicles, and mobile devices, which often includes locating their owners too. LBSs are almost everywhere, ranging from exploring *Point-of-Interests* (POIs) to geosocial networking and location-based commerce. As a matter of fact, among the ≈1M application available on Google Play, 24% of them request access to the user's precise location [20]. Besides, a typical Android device may share accurate location coordinates up to 5398 times in just two weeks; with the presence of just ten of the most popular apps, and with or without the explicit consent of its owner [3]. Furthermore, 70% of smartphone users have at least 11 downloaded applications. Moreover, a study conducted by the US Census Bureau revealed that more than 50% of users are willing to share their exact location [21].

The issue is not just about the location coordinates themselves; it is about their value to LBSs and other third parties. For instance, location is a valuable asset in an individual re-identification process [19]. However, as long as the location data does not link to an individual identity, it may prove useful in various cases. For example, in Canada, police analysts were able to build a picture of what was going on in downtown Ottawa during the October 2014 attacks, by using specific Twitter hashtags and location tools [23], illustrates an example of positive use of location data.

To use LBS features, a user needs to provide accurate geographic coordinates. In other words, LBS users do not have other choices but giving up their geographic coordinates, even when they are aware of the related privacy risks. For example, when 68% of mobile users are concerned about privacy and security on their devices [6], 74% of them still use LBSs to get location-based routes and information [27]. In 2015, The European Global Navigation Satellite Systems Agency, also known as The European GNSS Agency (GSA), released a report about LBSs and their usage [11]. Among its key findings, the report affirms that mobile applications relying on location information hit almost 3 billion downloads from both Android Play and Apple App stores.

Similarly, most of the recent mobile devices include support for numerous positioning systems such as GPS, Beidou, GLONASS, and SBAS, which improves location accuracy beyond what conventional GPS receivers can provide. Moreover, knowing that only 35% of mobile users think of turning off location services on their devices [27], suggests that the amount of user-generated location-based content is considerably huge. Many companies raise their revenues from data warehouses and analytic tools [2].

Location information itself is considered sensitive, for instance, four distinct spatiotemporal transactions are enough to identify 90% of LBS users [7]. Furthermore, collecting and processing location data on a regular basis may lead to infer one's private information such as the home or work locations, sexual preferences, or religious inclinations [4]. However, the benefits that LBS may provide cannot be ignored; one cannot just wipe out all location-based applications from his device. It is up to researchers and service providers to ensure the user's privacy on LBSs, either by building privacy-aware applications or by supplying protection mechanisms that meet user expectations.

Even when the existing protection models and mechanisms may guarantee good location protection, the fact that continuous requests are not independent, and the user's data is not isolated from location data may foil many Location Privacy Preserving Mechanism (LPPM from here onward). Moreover, performing privacy-preserving operations on geographic coordinates may lead to a notable quality loss. Thus, the balance between preserving users' privacy, and ensuring high accuracy from their location data is one serious challenge in today's applications.

Similarly, the technological advances in today's LBSs, especially in machine learning and inference technologies, put into question the effectiveness of abstracting location privacy to geographical coordinates, or single location-based request. LBSs can access, collect and store data that could help pinpoint to the exact user whereabouts. An example of the advancement achieved in location-related intelligence is the work proposed by Weyand *et al.* where the authors succeeded in identifying the location of photos just by analyzing them [25]. An approach entirely based on convolutional neural networks attests the progress achieved in this field.

We discuss in the next section the context of LBSs in more details, along with the significant privacy issues associated with their usage. Then, we represent the paradigms used in today's protection mechanisms. We also discuss the effectiveness of the latter and their potential shortcomings in the near future.

2 Location and Privacy

As stated by Bettini, "A privacy threat occurs whenever an unauthorized entity can associate with high probability the identity of an individual with private information about that individual" [5]. Accordingly, a privacy threat in LBS is characterized by the use of one's location to increase the probability of their identification.

We describe two scenarios in the context of this paper which involve interactions between users and LBSs. They are used to discuss our point of view regarding privacy in LBSs. It is assumed that the users are equipped with high-end devices, (*i.e.* GPS and WiFi enabled mobile devices) and can access various services offered by different service providers. Figure 1 illustrates the possible services that users can access nowadays via their smart mobile devices.

The context of this paper is LBSs, which are application services that rely on the location information transmitted by users. We abstract away from communication services, which include telephony and internet services, and have to determine the mobile device availability and position as a part of their base architecture. Communication services have to determine in which cell the mobile device is located so it can be served by the respective base transceiver station (BTS) [12]. Accordingly, we set in the following two scenarios that describe hypothetical LBS use cases that are not far from reality and may occur to any LBS user.

Scenario 1. Alice has an appointment with a doctor that she never visited before. The doctor is a specialist in treating diabetes, and his office is in a region

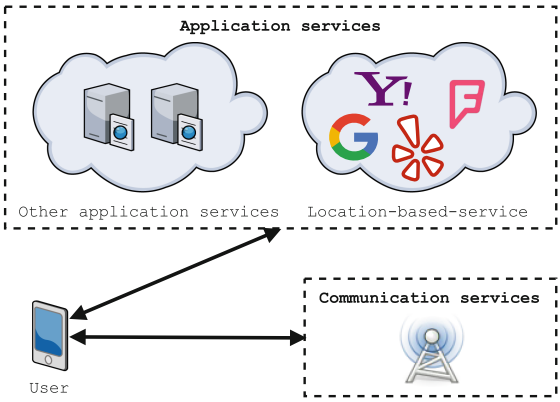

Fig. 1. Accessible services via smart mobile devices

that Alice is not very familiar with it. The day of her appointment, Alice takes her car and drives to the vicinity of the office. Once there, she cannot locate the doctor's office and thinks of using her smartphone to use her favorite LBS to find it. Although she knows that using an LBS would get her to the doctor faster, Alice is concerned about her privacy and knows that she has to disclose her identity and location to the LBS along with her request of finding the diabetes physician.

Scenario 2. Alice decides to use LBS to locate the doctor's office since she is afraid of being late. When she arrives, she meets Bob, a computer engineer who works on software development. While they are chatting in the waiting room, Alice mentions the fact that she is not comfortable with sharing her information to application services, especially geographical coordinates. Bob agrees with Alice's point of view and affirms that, as he works on collecting data from users, he can ensure her that the actual information disclosure is far beyond her perception. Bob gives her the example of storing the details of appointments in her device's calendar along with using an LBS to locate her appointments' locations. Alice realizes that even if she preserves her geographical coordinates, an installed LBS application still can access and correlate other sensitive data, such as photos, calendar events, and contacts.

While hypothetical, the above scenarios are close to real-world situations and may happen to any LBS user, even when using one LBS only. Thus, identifying the LBS-related privacy issues from the previous scenarios helps in setting the following requirements that an efficient LPPM should ensure.

- ***Strong location privacy.*** To efficiently protect user's location privacy, LBSs should not be able to identify or infer his exact location.
- ***Maximum data utility.*** The users are using LBSs to get location-enhanced data and provide them with inaccurate or misleading information thereby making the LBS useless. Consequently, ensuring high accuracy and maximum utility is a crucial requirement for an efficient LPPM.

– ***Efficiency.*** The LPPM should be able to deploy and run smoothly on mobile devices, along with keeping adequate run time, computation, and bandwidth efficiency factors. Similarly, the execution on the LPPM should not affect the latency and the response time when using LBSs.

Given the current LBS applications, the above requirements are fundamental to any proposed LPPM. Today's LBSs are beyond using location data only, and their ability to learn users' behaviors is evolving quickly. For example, consider an LBS user Alice who is concerned about her privacy protection and uses a given LPPM to achieve that. The latter tries to make Alice's location-based requests indistinguishable among a set of locations (*Confusion paradigm*). However, the LBS can access multiple data types on Alice's device, and can eventually identify if the request comes from Alice by correlating current and past data. Table 1 lists the required permissions in some of LBS mobile applications on Android.

Table 1. Examples of the required permissions in LBS mobile application

LBS application	Version	Common permissions	Other permissions
Google Maps	9.54.1	Location Storage Stored accounts	Camera Contacts
Yelp	9.12.0		Camera Contacts Microphone
Foursquare	2017.05.15		Contacts WiFi and Bluetooth information
Tinder	7.2.0		Call information Device and app history Device ID
Pokémon GO	0.63.4		Camera Contacts

The examples specified in Table 1 illustrate LBSs from different classes, and they sample what most of today's LBS applications collect from users' devices. More precisely, an LPPM that abstracts away from any background knowledge acquired by LBSs can be foiled, and eventually, fails to achieve its purpose of protecting location privacy.

3 Related Work Overview

Preserving privacy in LBSs implies that the users' exact locations must not be, in any case, disclosed or inferred. This rule, which might look simple, has driven many researchers to deeply explore the related issues, and produce numerous

valuable work on privacy threats in LBSs. From the perspective of this paper, we discuss the related work according to the paradigms on which existing privacy mechanisms have been built. Regardless of the adopted privacy metric (*e.g. k*-anonymity, differential privacy), we discuss in the following the two main classes of paradigms used in almost any LPPM.

3.1 Transformational Paradigms

Obfuscation. Mechanisms using this class of paradigms aims to hide the user's true location inside a larger area. As defined in [9], the main purpose of location obfuscation is deliberately degrading the quality of information about an individual's location in order to protect their location privacy. Let M be the mechanism using the obfuscation as its transformation paradigm, and $\mathbb{E}^2$ the space on which location operations are executed. The obfuscation region r is defined as follows:

$$M(loc) = r \in \mathbb{E}^2 \quad \text{with} \quad loc \in M(loc)$$

Substitution. In this class of transformations, the mechanism maps the user's true location to a different nearby location. As a result, a substitute location loc' is reported to the LBS instead of the user's true location loc. Let M be the mechanism using the substitution as its transformation paradigm, and $\mathbb{E}^2$ the space on which location operations are executed. The substitute location loc' is defined as follows:

$$M(loc) = r \in \mathbb{E}^2 \quad \text{with} \quad loc \in M(loc)$$

Confusion. The user's real location is confused when it is contained in a set of dummy locations in the aim of hiding it [17]. In other words, a mechanism using confusion paradigm maps the user's actual location loc into a set of n locations of which one is the exact location. Let M be the mechanism using the confusion as for its transformation paradigm. The set of confused location is defined as follows:

$$M(loc) = \{loc_i\}_{i \in [1,n]} \quad \text{such that} \quad \exists loc_i = loc$$

Suppression. Also known as *invisible cloaking*, the mechanisms using this class of transformations withdraw the LBS requests and prevent reporting any location coordinates in the presence of some predefined conditions. Let M be the mechanism using the suppression as its transformation paradigm; the suppression transformation is expressed by:

$$M(loc) = null$$

3.2 Collaborative Paradigms

Collaborative mechanisms ensure co-utility among users, and it has been proven that in a privacy-aware setting, not only they can provide strong privacy guarantees, but also more likely to be adopted by rational users [8]. They are based on forwarding location-based requests from one user to another such that the final request set R sent to an LBS from a collaborative network composed of n users is:

$$R = \{r_i\}_{i \in [1,n]} \quad \text{such that} \quad \exists r_i = r_u$$

The use of the discussed paradigms depends on the privacy goals of a mechanism and the properties of the LBS under consideration. As listed in Table 2, some paradigms outperform in the case of sporadic requests (*e.g.* Location-based search engines), others are more suitable for continuous requests (*e.g.* Navigation services). Mechanisms based on suppression paradigms are more useful in interrogation-based LBSs where the user initiates the request, and they cannot be used in transaction-based LBSs where the request is first sent by the service (*e.g.* Crowdsensing services). The table also mentions the effectiveness of the paradigms in both privacy protection and utility.

Table 2. Summary of location privacy preservation models

LPPM	LBS Properties						Effectiveness	
Paradigms	Direction		Request frequency		Content		Privacy	Utility
	Interrogation	Transaction	Sporadic	Continue	Location	Other		
Transformational paradigms								
Obfuscation	•	•	•	•	•		•	
Substitution	•	•	•		•		•	
Confusion	•	•	•		•			•
Suppression	•		•		•		•	
Collaborative paradigms								
Collaboration	•	•	•		•	•	•	•

4 Discussions

Location data has always been considered as personal information or at least known only by acquaintances. The negative consequences of its disclosure cannot be neglected. Besides, the combination of location data with other personal information can lead to precisely identify individuals by potentially malicious parties.

The current state of LBSs reveals several privacy-related issues. For instance, location prediction on social networks such as Twitter represents one of them [26]. Location prediction combines the inaccurately reported positions with social content (*e.g.* posts, photos) to provide accurate coordinates. Moreover, a study conducted by Haffner *et al.* attested that the location data gathered from social networks seem to be more accurate than volunteered geographic information such as OpenStreetMap [14].

Location prediction is not related to social networks only, for instance, the navigation application Waze uses the mobility patterns of its users to provide traffic predictions. Exact location prediction is the primary feature of LBSs to provide useful data. However, the more a position is accurate, the more the privacy is at risk.

Another emerging field that may imply additional privacy protection measures is the ability to identify the location using photos on social media [24,25]. The user's photos on social networking platform can be used to identify their exact location using contextual information extracted from the photo itself (*e.g.* Buildings, Road signs, weather). As long as no protection mechanism analyzes photos for possible location identification, such technology makes current mechanisms completely useless. Users can disable location tracking, prevent any unwanted location disclosure, but this is not enough when it comes to content analysis.

One other questionable point is the effectiveness of the existing protection mechanisms. Most existing solutions focus on preserving privacy by ignoring the utility. As a result, some LBSs may end up good for nothing, for instance, navigation LBSs cannot provide directions if the location is not accurate. Nevertheless, preserving privacy alone is a complicated issue given the computational and learning capabilities that current LBSs possess. Thus, the consideration of utility adds a dimension that must be treated independently.

Even when the existing protection mechanisms can guarantee privacy protection, the lack of severe measures for some LBS models may lead to privacy breaches and quality loss. In other words, if a user opts for various LBSs, which is often the case, they will be forced to select the same number of protection models to ensure the privacy protection and the service quality. Moreover, the absence of a global LBS model behind the existing solutions makes them unable to achieve higher privacy guarantees. For instance, a user can obtain rigorous privacy guarantees when using a location-based social network with a protection mechanism. However, using the same mechanism in a navigation service may be ineffective.

It is important to note the usefulness of current technologies in many aspects of our daily lives. However, the information they collect can be exploited and therefore cause harm to our privacy. An adversary can examine a user's data, analyze it, and create relevant information that could be used to generate behavioral models based on the user's location. For example, marketing companies, such as Urban Airship or others, now offer audience profiling tools that enable the integration of customer targeting capabilities based on their location-based data.

The issue of privacy in location-based services is far from being new. Nevertheless, the fast growth of both their users' adoption and their technologies makes the existing LPPMs either ineffective or complicated. While ineffective LPPMs are dismissed, complicated ones decrease the utility of LBSs. For instance, LPPMs based on differential privacy end up adding too much noise to the real position to the point the retrieved data from an LBS becomes completely useless.

We discuss in the next section the future of LBSs and the need for rethought LPPMs.

5 Future of Geolocation

A team from *Imperial College London* and *M Squared* have recently developed what they called "quantum accelerometer" [10]. The device measures movements and, unlike traditional accelerometers, it can accurately report positions. What makes it revolutionary is its autonomy, it does not rely on satellites or wireless networks to estimate its position. From a privacy perspective, this may make the control over location disclosure even harder. Cutting links with satellites will not be enough.

One other category that impacts the location as we know today is the Internet of Things (IoT). With already existing devices (*e.g.* smart watches, connected home appliances) and near-future launching plans (*e.g.* connected smart lens, health monitoring rings), the control over how location data is collected and used may become impossible. What is done today by switching off location tracking on a smartphone, could imply, soon, a whole set of settings and reading privacy agreements. Using multiple connected devices ensures high location accuracy on the one hand and facilitates privacy breaches on the other hand.

A report from *Reserach and Markets* predicts that revenues from location-enabled IoTs will reach $49 billion by 2021 [22]. The report also suggests that the significant growth of Low-Power Wide Area Network (LPWAN) technologies will help in connecting IoT devices more easily, and as a result facilitating location data collection. In a nutshell, LPWANs networks represent a type of wireless telecommunication wide area networks designed specifically to allow long-range communications at a low bit rate among IoT devices [1].

The bottom line is that location collection methods and techniques are changing and newly related privacy-issues are emerging. Today's protection mechanisms rely on satellites data and calculation power of smartphones. With auto-locating devices and limited IoT resources, the challenge becomes even harder. Not to mention the multitude of connected devices that implies the need for one protection system that controls privacy over all of them at once.

6 Conclusion

The fact that LBSs are invading our lives on a daily basis cannot be overlooked; it is thanks to their ease of use and convenience that the number of their users is increasing exponentially. However, this adoption leads to severe risks regarding users' privacy. The aggregation and analysis of location data have become even more accessible, and can certainly be refined when position history and tracking.

The usefulness and convenience offered by LBSs is the primary reason behind this adoption. In the majority of cases, users adopt an LBS because they need to use it. Therefore, a radical "abandon LBS" solution is not applicable. Users need to use LBS, but they also need to protect their privacy.

We discussed in these paper LBS models and privacy-preserving paradigms, along with significant challenges when it comes to providing the optimal protection.

References

1. Adelantado, F., Vilajosana, X., Tuset-Peiro, P., Martinez, B., Melia-Segui, J., Watteyne, T.: Understanding the limits of LoRaWAN. IEEE Commun. Mag. **55**(9), 34–40 (2017)
2. Aïmeur, E., Lawani, O., Dalkir, K.: When changing the look of privacy policies affects user trust: an experimental study. Comput. Hum. Behav. **58**, 368–379 (2016)
3. Almuhimedi, H., et al.: Your location has been shared 5,398 times! A field study on mobile app privacy nudging. In: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, pp. 787–796. ACM (2015)
4. Andrés, M.E., Bordenabe, N.E., Chatzikokolakis, K., Palamidessi, C.: Geo-indistinguishability: differential privacy for location-based systems. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, pp. 901–914. ACM (2013)
5. Bettini, C.: Privacy protection in location-based services: a survey. In: Gkoulalas-Divanis, A., Bettini, C. (eds.) Handbook of Mobile Data Privacy, pp. 73–96. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-98161-1_4
6. Clarke, N., Symes, J., Saevanee, H., Furnell, S.: Awareness of mobile device security: a survey of user's attitudes. Int. J. Mob. Comput. Multimed. Commun. (IJMCMC) **7**(1), 15–31 (2016)
7. De Montjoye, Y.A., Radaelli, L., Singh, V.K., et al.: Unique in the shopping mall: on the reidentifiability of credit card metadata. Science **347**(6221), 536–539 (2015)
8. Domingo-Ferrer, J., Martínez, S., Sánchez, D., Soria-Comas, J.: Co-utility: self-enforcing protocols for the mutual benefit of participants. Eng. Appl. Artif. Intell. **59**, 148–158 (2017)
9. Duckham, M., Kulik, L.: A formal model of obfuscation and negotiation for location privacy. In: Gellersen, H.-W., Want, R., Schmidt, A. (eds.) Pervasive 2005. LNCS, vol. 3468, pp. 152–170. Springer, Heidelberg (2005). https://doi.org/10.1007/11428572_10
10. Dunning, H., Angus, T., Martin, M.: Quantum compass could allow navigation without relying on satellites, November 2018. https://goo.gl/Dwr8ed. Accessed 13 Nov 2018
11. European GNSS Agency: GNSS market report: location-based services, March 2015. https://goo.gl/FBvrRa. Accessed 25 Nov 2018
12. Frattasi, S., Della Rosa, F.: Mobile Positioning and Tracking: From Conventional to Cooperative Techniques. Wiley (2017)
13. Griffin, A.: Google stores location data even when users have told it not to, August 2018. https://goo.gl/4erH3v. Accessed 13 Nov 2018
14. Haffner, M., Mathews, A.J., Fekete, E., Finchum, G.A.: Location-based social media behavior and perception: views of university students. Geogr. Rev. **108**(2), 203–224 (2018)
15. Howley, D.: Facebook reveals 50 million accounts affected by security breach, September 2018. https://goo.gl/ETjrpV. Accessed 13 Nov 2018
16. Kelly, G.: eBay suffers massive security breach, all users must change their passwords, May 2014. https://goo.gl/42wSHH. Accessed 13 Nov 2018

17. Kido, H., Yanagisawa, Y., Satoh, T.: An anonymous communication technique using dummies for location-based services. In: Proceedings. International Conference on Pervasive Services, ICPS 2005, pp. 88–97. IEEE (2005)
18. Larson, S.: Every single Yahoo account was hacked - 3 billion in all, October 2017. https://goo.gl/bXZbru. Accessed 13 Nov 2018
19. Li, G.: A new reidentification method for location-based social networks. IEEJ Trans. Electr. Electron. Eng. **14**(3), 499–500 (2019)
20. Olmstead, K., Atkinson, M.: Apps permissions in the Google play store, November 2015. http://www.pewinternet.org/2015/11/10/apps-permissions-in-the-google-play-store/. Accessed 25 Nov 2018
21. Olmsted-Hawala, E., Nichols, E.: Willingness of the public to share geolocation information in a us census bureau survey. Soc. Sci. Comput. Rev. (2018). https://doi.org/10.1177/0894439318781022
22. Research and Markets: Location-based IoT and geo analytics market outlook and forecasts 2017–2022, April 2017. https://goo.gl/fHdpi8. Accessed 13 Nov 2018
23. Stewart, E.: Live-tweeting a terrorist attack: how the public's posts can help in an emergency, April 2016. http://www.rcmp-grc.gc.ca/en/gazette/live-tweeting-a-terrorist-attack. Accessed 25 Nov 2018
24. Wang, K., Huang, Y.H., Oramas, J., Van Gool, L., Tuytelaars, T.: An analysis of human-centered geolocation. In: IEEE Winter Conference on Applications of Computer Vision (WACV), pp. 2058–2066. IEEE (2018)
25. Weyand, T., Kostrikov, I., Philbin, J.: PlaNet - photo geolocation with convolutional neural networks. In: Leibe, B., Matas, J., Sebe, N., Welling, M. (eds.) ECCV 2016. LNCS, vol. 9912, pp. 37–55. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-46484-8_3
26. Zheng, X., Han, J., Sun, A.: A survey of location prediction on Twitter. IEEE Trans. Knowl. Data Eng. **30**(9), 1652–1671 (2018)
27. Zickuhr, K.: Location-based services (2013). https://goo.gl/JYcjeq. Accessed 25 Nov 2018