IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 20, 2018, accepted March 27, 2018, date of publication April 2, 2018, date of current version April 23, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2822260

Location Privacy and Its Applications: A Systematic Study

BO LIU[1], (Member, IEEE), WANLEI ZHOU[2], (Senior Member, IEEE), TIANQING ZHU[2,3], LONGXIANG GAO[2], (Member, IEEE), AND YONG XIANG[2], (Senior Member, IEEE)

[1]Department of Engineering, La Trobe University, Melbourne, VIC 3086, Australia
[2]School of Information Technology, Deakin University, Melbourne, VIC 3125, Australia
[3]School of Mathematics and Computer Science, Wuhan Polytechnic University, Wuhan 430023, China

Corresponding author: Tianqing Zhu (t.zhu@deakin.edu.au)

This work was supported in part by the National Natural Science Foundation of China under Grant 61502362 and in part by the Australia Research Council Linkage under Grant LP170100123.

ABSTRACT This paper surveys the current research status of location privacy issues in mobile applications. The survey spans five aspects of study: the definition of location privacy, attacks and adversaries, mechanisms to preserve the privacy of locations, location privacy metrics, and the current status of location-based applications. Through this comprehensive review, all the interrelated aspects of location privacy are integrated into a unified framework. Additionally, the current research progress in each area is reviewed individually, and the links between existing academic research and its practical applications are identified. This in-depth analysis of the current state-of-play in location privacy is designed to provide a solid foundation for future studies in the field.

INDEX TERMS Location privacy, location-based service, mobile applications.

I. INTRODUCTION

Global positioning systems (GPSs) are now a standard component in most cell phones, and their ubiquity is driving high growth in location-based information services (LBSs). According to statistics [1], in 2016, there were nearly 200 million LBS users in the US. Inevitably, this upward trend will continue since LBSs fill many useful and interesting needs in a wide range of areas. Mobile social networks [2] [3], navigation [4], finding places of interest (POI) [5], sports and health assistants [6], and augmented reality (AR) games [7] are just a few of the practical applications that have benefited from LBSs. In fact, for many businesses and government agencies, LBSs have become a critical part of deriving real insights from data tied to the specific locations where an activity takes place. However, accessing personal location data, even with permission, raises severe privacy concerns for most users and, therefore, effective privacy preservation is foremost for LBS applications.

As a result, scholars have undertaken a great deal of research into ways of preserving the privacy of user locations. Various methods have been proposed, such as cryptography [8], anonymity [9] [10], obfuscation [11] [12] and caching [13] but, despite these efforts, there are still some obstacles to the progress of location privacy research:

- It is difficult to make comparisons between the different location privacy preservation mechanisms (LPPMs) because there is little consensus on the definition of location privacy or the best metrics to use to measure privacy levels.
- The gap between theory and practice is vast, with little analysis on how to implement LPPMs in real-world applications.

In this context, a systematic study of location privacy in all its related aspects is essential to future research efforts in this important topic. This includes a definition of privacy, the role of adversaries, the metrics used to measure privacy levels, and the LPPMs used along with how and where they are applied.

This study is not the first or only attempt to comprehensively survey location privacy. However, previous surveys have tended to focus on privacy preservation schemes [14] [15] [16] [17] [18] [19] [20], or are limited to a particular kind of network architecture [21] [22] [23] [24]. Shokri *et al.* [25] were the first to publish a unified framework of location privacy. Their review included various LPPMs and a qualitative comparison of three metrics for measuring location privacy: uncertainty, errors, and k-anonymity. The results show that entropy and k-anonymity are inadequate for measuring location privacy. Then in [26] the authors jointly

2169-3536 © 2018 IEEE. Translations and content mining are permitted for academic research only.
Personal use is also permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

consider obfuscation and anonymization methods, developing generic attacks that can be used against any LPPM.

Both these works only focus on one or two aspects of location privacy, and both lack analysis of the connections between attacks, LPPMs, privacy metrics, and a definition of location privacy. In addition, newer methods based on caching [13], differential privacy (DP) [27], game theory [28] [29], machine learning [30], etc., were not included in their literature reviews.

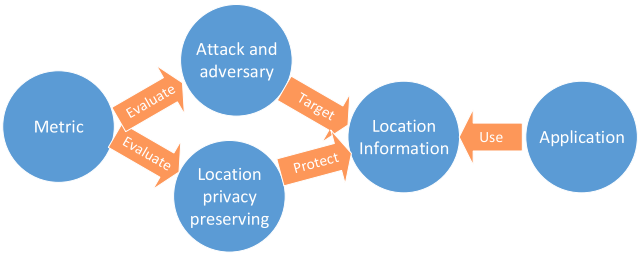


FIGURE 1. Connections of different aspects of the location privacy.

To overcome these obstacles, this study provides an updated and integrated framework for location privacy research. It includes location privacy definitions, and reviews of attacks and adversaries, LPPMs, location privacy metrics, and the applications that rely on location privacy. In addition, we analyze the relationships between the different aspects of location privacy (Fig. 1)- for example, the types of attacks that target particular attributes of location privacy but can be prevented by a certain type of LPPM or evaluated with a certain metric.

The main contributions of this paper follow.

- We define location privacy using a generic definition that covers all aspects of a user's location information including identity, position, and trajectory. In addition, we analyze the special characteristics of location privacy data.
- Four aspects of attacks and adversaries are examined to provide a comprehensive description of adversaries and their behavior: methods of obtaining location information, adversarial knowledge, methods of attack, and targets of attack. New and emerging trends in attacks, such as deep learning attacks, are also discussed.
- The milestone LPPMs are analyzed along with an investigation of the different LPPM categories and the evolution of logic inside each category.
- We summarize the most commonly-used location privacy metrics and identify the connections between those metrics and the LPPMs.
- We explore the location privacy issues associated with practical implementation, including the type of location information each LBS uses, the potential applications for each type of LPPM, and the current research progress into these methods.
- The study concludes with a discussion on the likely directions of future research in location privacy.

Through this comprehensive overview, we hope to provide a foundation for future studies in this area.

The rest of the paper is structured as follows. Section II presents our definition of location privacy. In Section III, we model the four aspects of adversaries and attacks. We classify and compare existing LPPMs in Section IV, followed by an overview of privacy metrics in Section V. In Section VI, we present the current status of location privacy in terms of real-world applications, and future directions of research are discussed in Section VII. Finally, we conclude our work with a summary in Section VIII.

The abbreviations used in this paper are listed in Table 1.

TABLE 1. Summary of important abbreviations.

LBS	location-based service
LBA	location-based application
TTP	trusted third party
AR	augmented reality
LPPM	location privacy preservation mechanism
POI	place of interest
GPS	global positioning system
MSN	mobile social network
MCS	mobile crowd sensing
DP	differential privacy
PIR	private information retrieval
SQL	service quality loss

II. SYSTEM MODEL OF LOCATION-BASED SERVICES AND THE DEFINITION OF LOCATION PRIVACY

LBSs pose the risk of location privacy disclosure because they rely on a variety of location information to provide their services. This section begins by introducing a generic system model of an LBS. Then, location privacy is defined within in this scope.

A. LOCATION-BASED SERVICES

Fig. 2 illustrates the general structure of an LBS. It contains the following components:

- A positioning system: GPS satellites are the most widely-used positioning system. Cellular base stations and Wi-Fi routers can also be used as locating devices.
- Users: Most LBSs are distributed on mobile phones. However, LBSs are also frequently found in wearable devices and vehicles.
- Networks: Communication networks, including wireless local networks and cellular networks, are typically the first hop in the data transmission. Data is then usually transmitted over the Internet.
- LBS server: The LBS server responds to user queries and is usually operated and maintained by the LBS provider.
- Content/Data Provider: LBSs require massive amounts of data, such as POIs and maps. Some LBS providers own their own data and content, while others use a third party to provide this service.
- Location privacy server: The location privacy server executes the privacy preservation algorithms, such as

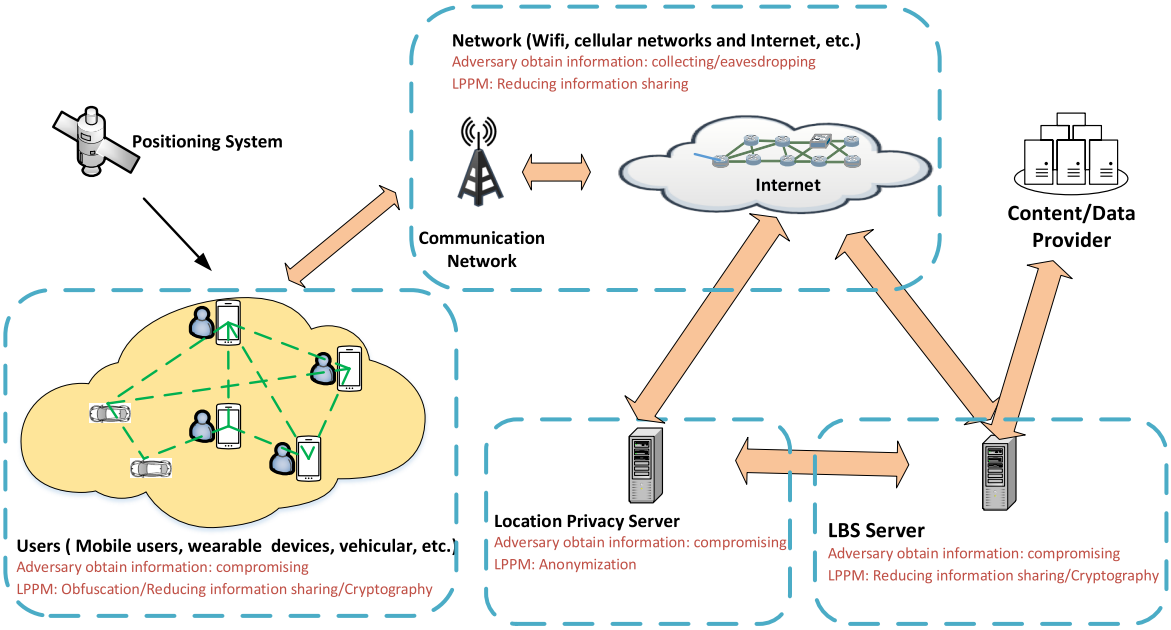


FIGURE 2. System model of location based services.

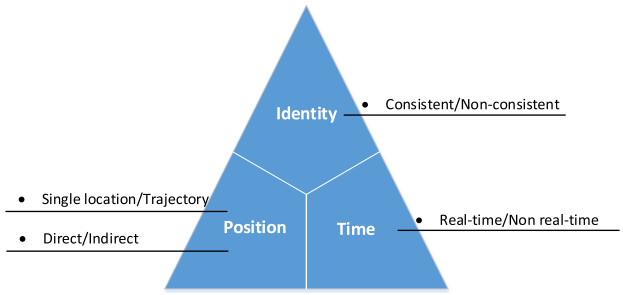


FIGURE 3. Three attributes of the location information.

anonymization and encryption. This server can either be owned and operated by the LBS provider or by a third party.

The structure of the LBS dictates, in part, the possible types of attacks and adversaries a provider may confront. A more detailed discussion on this is provided in Section III.

B. REPRESENTATION OF LOCATION INFORMATION

From a privacy perspective, the location information in LBSs is not just a set of coordinates or the name of a place. It may also include the user's identity, spatial information (position), and temporal information (time), as shown in Fig. 3. Hence, a user's location information can be defined as a tuple $<$ *identity*; *position*; *time* $>$ [31] [19]. Each of these attributes can take different forms, as summarized in the following.

1) IDENTITY

Identity is a user's name, email address, or any feature that makes a person distinguishable from another. In LBSs, identities can be either consistent or non-consistent [32].

Some LBSs require consistent user identities. For example, Pokemon Go requires its users to log in, while WeChat's "find my nearby friends" function requires users to continuously provide their location information along with their WeChat ID [3].

Other LBSs do not require consistent user identities, or even the user's identity at all. For example, one can use Google Maps to find nearby restaurants anonymously or with a pseudonym.

An email address is the most common consistent identity required by LBSs. However, email addresses are an integral part of a user's private information and can easily be used to conduct context linking attacks.

2) SPATIAL INFORMATION (POSITION)

Spatial information is the primary means of determining a location. Locations can either be described as a set of coordinates (e.g., longitude and latitude), or by some other form of information that can be linked to a location, such as a shop name. The different types of spatial information can be loosely divided into two categories:

Single locations and trajectories: Single locations are scattered and do not correlate to other locations. A trajectory is a group of locations with strong correlations, for example, a person trace.

Direct locations and indirect locations: Traditional LBSs, such as a "check-in" or "nearby-POI" services, use direct locations defined by GPS coordinates. Whereas, more recently, geo-social discovery services, which use indirect locations, have been rapidly growing in popularity. WeChat and Facebook contain good examples of these new types of services, where connections among users are explicitly

established on-the-spot based on physical proximity. Rather than pinning down a user's exact location on a map, proximity information is provided instead, such as ''Tom is within 3 miles'' [30].

3) TEMPORAL INFORMATION (TIME)

In addition to identity and location information, some LBSs also associated a time stamp with a location. Again, temporal information can be divided into two groups:

Non-real time: Some applications, such as Fitbit tracking, publish location or trajectory information afterward.

Real-time: Real-time privacy protection is more challenging than non-real-time protection because the scalability requirements in real-time privacy preservations become a much more important factor. Further, global optimization is very difficult with real-time information due to the highly dynamic and uncertain movements of users [32]. Examples of LBSs that use real-time location information include navigation and AR games.

C. THE DEFINITION OF LOCATION PRIVACY

Thus, location privacy can be defined as the protection of these three attributes of a person's location information. Blumberg and Eckersley [33] use the following definition:

Location privacy ''is the ability of an individual to move in public space with the expectation that under normal circumstances their location will not be systematically and secretly recorded for later use''.

They also argue that there is no absolute location privacy, because:

''...when you leave your home you sacrifice some privacy. Someone might see you enter the clinic on Market Street, or notice that you and your secretary left the Hilton Gardens Inn together.''

According to this definition, location privacy has two main features: the individual's expectation of ''normal circumstances'', and the way the information is collected and used. However, a person's expectation of location privacy can change over time, especially with the rapid development of information technology and the dramatic increase in the amount of location information that is used in everyday life. Additionally, the ways we collect and use location information has also changed. Today, personal information is more often collected quietly by inconspicuous devices, such as mobile phones, RFID tags, and cameras [34]. Moreover, newly emerging technologies, such as machine/deep learning and face-recognition, have also changed how location data can be used to derive more sensitive personal information.

Therefore, to evaluate the privacy of a location, its key factors must be defined from the users' point of view:

- How: how is the information revealed? Is it revealed secretly or publicly? Is it encrypted or not? And how will the information be used?
- What: what kind of information is revealed? Is it a set of coordinates, at a particular time, and with my identity attached? Are these attributes precise or coarse?

These two key factors also form the basis of our investigation into the features of attacks and adversaries in the next section of the paper.

D. LOCATION PRIVACY VS. DATA PRIVACY

Location privacy is a subcategory of data privacy. Among the different types of personal data categories, the risks of unsanctioned disclosures of financial and medical records are well known. However, risks associated with location are no less grave for the following reasons:

- Identity inference: Location data holds a unique capacity to link disparate datasets in a way that can reveal personally identifiable information through inference. And these links only rely on an understanding of the relationships between data and human activity.
- Profiling completeness: User locations typically contain POIs, such as hospitals and restaurants. Thus, one may be able to gain a deeper understanding of user behavior in the real world and use that data to predict future activity. The ability of location information to ''connect the dots'' almost automatically results in a much more complete profile of an individual or organization than the base data contains.

Location data also holds some distinguishing characteristics. Location data is typically:

- Massive: Using an LBS generates enormous amounts of location data, no matter the form.
- Highly correlated: A real-world location dataset often exhibits strong coupling relations; locations are often correlated, and these correlations may disclose more information than expected.
- Dynamic: The data can change quickly over time.
- Unequal in importance: From a user's point of view, their privacy requirements differ from location to location. For example, most people care very little about exposing the location of a shopping center visit, but care very much about keeping their home and workplace secret.

These features require special attention when conducting location privacy studies.

III. LOCATION ATTACKS AND ADVERSARIES

An adversary aims to collect location information and use it for their benefit. Based on the two key factors of location privacy, an adversary and their attack can be characterized by ''how'' they obtained the information, ''how'' the attack is launched, ''what'' information or knowledge they obtained, and ''what/who'' their target is. Fig. 4 illustrates this four-part model of an adversary and an attack. Each aspect of the model will be analyzed in detail in this section.

A. LOCATION INFORMATION OBTAINING METHODS

As shown in Fig. 2, the three main parties in an LBS system are the users, the servers, and the networks. Each party can be attacked, and each attack can be measured and categorized by its victim and level of danger.

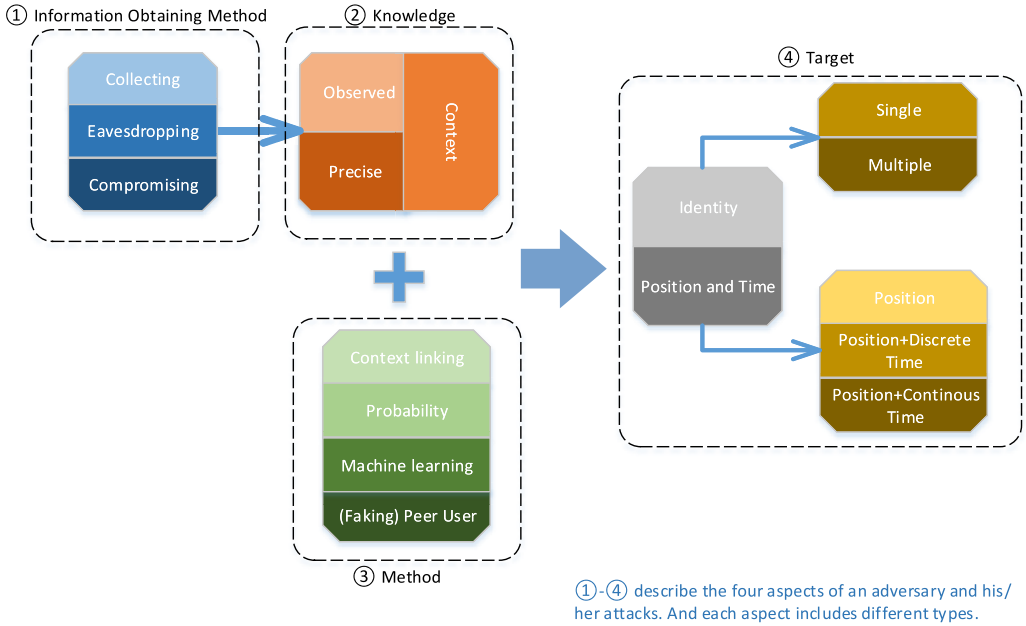


FIGURE 4. An overview of the location attacks and adversaries.

1) Collecting shared or published location information, historical statistics, or distributions. Some attacks can be as simple as collecting published data using tools like a Web Crawler.
2) Eavesdropping on a network (communication channel) can expose the data traffic between the server and client or between clients (e.g., peer-to-peer networks), especially with the wireless networks.
3) Compromising the server or the client through a hack that extracts any information an adversary wants.

B. TYPES OF ADVERSARIAL KNOWLEDGE

Once an adversary has acquired some location information, through whatever means, they may hold the necessary knowledge to carry out a location attack. However, the power of this knowledge depends on whether it has been processed through a privacy preservation scheme.

- Observed location information has been preprocessed by the user, a third party privacy server, or the service provider before being divulged. It may still be vulnerable to exploitation, but is less vulnerable than precise information.
- Precise location information has not been processed and is vulnerable to compromise and hacks.

In addition, an adversary may have other knowledge that can be used to help breach location privacy. This additional knowledge is referred to as:

- Context knowledge: any information that could be used by an adversary to help reveal the location information of a user.

Examples of contextual knowledge include: 1) the number of users in an area at a given time; 2) the relationships between different users; 3) the relationships between a user's identity and their location; 4) the location restrictions of an area, such as road networks and POIs; 5) the statistical distributions or probabilities associated with a location (e.g., people tend to stay home at night); and 6) social event information (e.g., well-publicized events held by, say, a celebrity or museum).

C. ATTACK TARGETS

The first type of attack is the self-explanatory *identity attack*. *Localization attack* combine spatial and temporal information as targets because this information is often highly related.

1) IDENTITY ATTACK

Identity attacks, also known as deanonymizing attacks seek information for the purposes of determining a target's identity. Examples of these types of attacks include:

- Personal identification attack (single identity attack): identifying a user based on their home address [35], or determining a person's gender and education, for example, through an anonymous trace [30].
- Meeting Disclosure Attacks/Aggregated Presence Attack (multiple identity attacks): inferring the relationship between two people or an aggregated property, for example, whether two people met on a certain day or the approximate number of people visiting a Pokemon Go stop.

2) LOCALIZATION ATTACK

Localization attacks focus on determining *position* and *time* information. Some examples follow.

- Sensitive place attacks (position attack): identifying important locations, such as home and work [36] [37].

- Presence and absence disclosure attack (position and discrete time attack): determining whether or not a user is present at a place at a specific time. For instance, empty homes are good targets for burglary; physically attacking a person requires you know where they are [38] [39].
- Tracking attack (position and continuous time attack): assembling a partial or entire sequence of the events to develop a user trace. This kind of adversary is generally known as stalking [40] [41] [42].

D. TYPES OF ATTACK METHODS

Lastly, adversaries can use different methods of attack.

- Context linking attacks: Most location attacks involve some contextual knowledge. Contextual knowledge is easy to combine with the observed location information to obtain a precise location for a target, for the purposes of conducting a localization attack. For instance, in a personal context linking attack [10], which can be used to reduce an obfuscated area to a specific location and then locate users by removing all the irrelevant areas. Contextual knowledge can also be combined with precise location information to conduct an identity attack. For example, if an adversary knows a person's home address and finds that address in a hospital's check-in list, the adversary can infer that their target is, or was, in that hospital at a specific time.
- Probability-based attacks: Probability distribution attacks [26] are based on gathered statistics about environmental contexts. A Markov chain model is widely used in these type of attacks. Using this method, an adversary can either perform a localization attack (location prediction [43]) or an identity attack (de-anonymization [44]). Strictly speaking, statistical information is actually a kind of contextual information; however, since exploiting probability theory is an important category of attacks, we have discussed it separately.
- Machine/deep learning-based attacks: Li *et al.* [30] proposed an approach to inferring user demographics in a mobile social network (MSN) based on machine learning. The type of demographic information included gender and education level, and their experiments demonstrated a 70% successful rate on a large real-world dataset. Murakami and Watanabe [45] proposed a learning method that uses tensor factorization to accurately estimate personalized transition matrices from a small amount of training data. The matrices are then used to launch a localization attack that can derive the actual location of a user at a given time from an obfuscated trajectory.

  In a recent work, Weyand *et al.* [46] showed that it is possible to determine the location of a photo by its pixels alone using a convolutional neural network.
- Collusion of malicious users attacks: Peers subscribing to the same LBS can either collude to launch attacks, or one adversary can create fake peers to obtain the information they seek. For example, Li *et al.* [47] created three fake anchor locations and used their corresponding distances to the target in an iterative trilateration based on a localization algorithm to obtain an inferred location.

E. EMERGING TRENDS

Big data and deep learning techniques are changing the landscape of location privacy. In particular, two attack trends have become more challenging than ever before - cross-database and platform attacks and deep learning attacks. Cross-database and platform attacks exploit the links between the location information in two different databases to infer sensitive information about their target. The unprecedented accuracy of deep learning methods is also posing significant challenges. For example, current deep learning-based methods are able to predict geolocations [46] from personal photos posted on social networks. These trends are likely to become the increasing focus of future research.

IV. LOCATION PRIVACY PRESERVATION MECHANISMS (LPPMS)

Shokri *et al.* [26] discusses LPPMs in two groups: obfuscation mechanisms and anonymization mechanisms. Our review of the literature reveals two further mechanisms, cryptographic mechanisms and shared information reduction mechanisms, creating four categories for existing LPPMs.

A. CRYPTOGRAPHIC MECHANISM

LPPMs based on cryptography use encryption to protect user positions. Mascetti *et al.* [48] proposed an approach to notify users when their friends, called buddies, are in proximity but without revealing the current user's position to the LBS server. To this end, the authors assume that each user shares a secret with each of his buddies through a symmetric encryption technique. Another approach proposed by Ghinita *et al.* [8] makes use of a private information retrieval (PIR) technique to provide location privacy. Through PIR, an LBS server can answer queries without learning or revealing any information about the query. PIR relies on an assumption of quadratic residuosity, which states that it is computationally hard to find quadratic residues in the modulo arithmetic of a large composite number for the product of two large primes. To deal with the problem of non-trusted LBS server infrastructures, Marias *et al.* [49] proposed an approach based on distributing the position information and secret sharing. The basic idea is to divide the position information into shares, which are then distributed among a set of (non-trusted) LBS servers. Hence, to reassemble the position information, the client needs to retrieve the shares from multiple servers. The advantage of this approach is that compromising one LBS server will not reveal the position information since it does not have all the necessary shares. However, the downside is that none of the LBS servers can perform computations that require all the position information, such as range queries.

Chen *et al*. [50] constructed a secure query protocol, where different data providers can use different secret keys to encrypt their data to prevent the location server from deducing the content of the query data.

The main concerns with cryptographic mechanism are their computational complexity and/or the requirement of cooperative servers. It is worth noting that this area of research has not seen any great breakthroughs for some time.

B. ANONYMIZATION MECHANISMS

These types of methods aim to break the links between identity and location information. They mainly fall into two categories: k-anonymity and mix-zone.

1) K-ANONYMITY

k-anonymity [10] [51] [52] [53] [54] achieves privacy preservation through generalization and suppression algorithms to ensure that one record can not be distinguished from $(k-1)$ the other records. A subject is considered k-anonymous if its location is indistinguishable from those of k - 1 other users.

The basic concept of k-anonymity [10] requires that the location privacy server is operated by a trusted third party (TTP). This trusted LBS server is aware of all precise user positions and acts as the anonymizer. Whenever a user needs to transmit their location along with a query, the TTP calculates a set of k users and reports an obfuscation area containing k positions including that of the querying user.

k-anonymity has been extended in two directions. The first direction attempts to avoid a single trusted anonymizer, either by employing multiple distributed servers [55] [56] or using peer-to-peer communication instead of a server [57]. The second direction constrains which users are included in k based on a set of conditions relating to the potential contextual knowledge an adversary may have. For example, p-sensitivity [58] aims to guarantee the key attributes have at least p different values within the k user set (i.e., an identity information constraint). l-diversity [59] [60] ensures that the location of the user is unidentifiable from a set of l different physical locations (i.e., a location information constraint). And historical k-anonymity [61] provides guarantees for moving objects (i.e., a time information constraint).

k-anonymization approaches are targeted at the applications that do not demand a true or pseudo identity, such as finding nearby gas stations or restaurants, or notifying a user of the sale price of items as they pass through a shopping mall. The basic concept is to break the link between the identity and the location by hiding this information among similar anonymous users. However, k-anonymization techniques are ineffective when the LBS relies on some form of identity information to deliver its services because this information in association with spatially cloaked regions is vulnerable to inference attacks [35] [62].

2) MIX-ZONE

Unlike k-anonymity, mix-zones can be used without user identity information. The first mix-zone approach was proposed by Beresford and Stajano [9]Here, the privacy of the user is maintained by constantly changing the user's name or pseudonym within a mix-zone. Since then, this method has been investigated in the context of several different applications. Ying *et al*. [63] proposed a dynamic mix-zone for location privacy in vehicular networks, which dynamically forms the mix-zone at the time the vehicle requests it. The MobiMix approach proposed by Palanisamy and Liu [62] is a mix-zone framework based on road networks that considers the anonymization effectiveness and resilience of timing and transition attacks. Lu *et al*. [64] incorporate pseudonym changes at social spots to achieve location privacy, while Gao *et al*. [65] uses a mix-zone framework that hides the exact location information within a designed trajectory mix-zone for mobile crowd sensing (MCS) applications. Xu *et al*. [66] treated the problem of optimal multiple mix-zones as a transportation problem and built a mixed-integer programming model with the objective of minimizing the amount of time the users' privacy level is lower than their privacy requirement.

Both the k-anonymity and mix-zone schemes require users to cooperate to reach a target level of privacy, thus inspiring research on incentives for cooperation. For example, Freudiger *et al*. [67] model the behavior of mobile nodes as pseudonyms change in a noncooperative game where each player aims to maximize their location privacy for minimum cost. Gong *et al*. [68] modeled user decision making about whether to change pseudonyms as a socially aware pseudonym change game. Auction-based mechanisms were designed in [69] to impel users to participate in pseudonym change. Gong *et al*. [70] assumed a general anonymity model that allows a user to have their specific anonymity set to a personalized level of location privacy using a social group utility approach.

Anonymization has been well-studied and applied to many different scenarios. However, this approach has also attracted some criticisms [71]. The main concern is that it is unreasonable to maintain the same level of anonymity in different contexts. For example, a group of users cooperating to achieve k-anonymity may either be near each other in a small place (e.g., a train station), or in the opposite situation and scattered across a large area. k-anonymity is satisfied in both cases, but it is clear that the users in the second case have better location privacy because an adversary would have more uncertainty about their exact locations. This example also implies that k is sometimes irrelevant to actual location privacy.

C. OBFUSCATION MECHANISMS

Obfuscation mechanisms encompass a range of methods that reduce the precision of location information. Some add dummy locations, others perturb (add noise), still others reduce the granularity of the information [26] [72] [73].

1) DUMMY LOCATIONS

The goal of position dummies is to mask a user's true position by sending multiple false positions (''dummies'') to

the LBS server together with the true position [11]. Since the dummy locations are randomly selected from the user's mobile device, this method does not require any trusted servers and is known to achieve good levels of privacy without loss of accuracy.

The classic dummy method only addressed single locations but has since been extended to trajectories. You *et al.*'s [74] method produces a user's dummy trajectories through random or rotating patterns. Specifically, the random pattern generates dummy trajectories beginning with the starting point and moving towards the destination. The rotating patterns cycle through a set of dummy user trajectories. Lei *et al.* [75] uses a rotation scheme to rotate a user trajectory that satisfies the distance deviation to make the actual user trajectory indistinguishable from the dummies.

Given that an adversary may have additional contextual knowledge, such as the map of a certain area, some research efforts have focused on improving the dummy location method to create dummies that not only are realistic but also cannot be distinguished from the user's true position. Krumm [76] faked a users' driving movements using a database of actual GPS tracks from 253 drivers. To make the model more realistic, they also compute the probability of a given position being a plausible start or end point. Chow and Golle [77] generated fake location traces by leveraging Google Maps. They add simulated stops and noise in the routes planned by Google Maps and output a fraction of the points according to the desired time range. Do *et al.* [78] proposed a dummy generation method using conditional probabilities to generate realistic false locations that are resistant to adversaries who have information about the user as well as external spatiotemporal knowledge. Hara *et al.* [79] proposed a method to generate natural dummies that considers the physical constraints of the real environment. Chen and Shen [80] proposed dummy selection using maximizing minimum distance (MaxMinDistDS) and a simplified version of MaxMinDistDS (SimpMaxMinDistDS) that takes both semantic diversity and the physical dispersion of locations into account.

2) LOCATION OBFUSCATION

Spatial obfuscation approaches attempt to preserve privacy by deliberately reducing the precision of the position information sent from the user to the LBS server and, in turn, to the client. A classic spatial obfuscation approach is the one presented by Ardagna *et al.* [12], [81], where a user sends a circular area instead of the precise user position to the LBS server. Gutscher [82] proposed an approach based on coordinate transformation, where the mobile device performs some simple geometric operations on their positions (e.g., shifting, rotating) before sending them to the LBS server.

These location obfuscation methods, designed to protect spatial information, led researchers to investigate ways of protecting temporal information. Hwang *et al.* [83] introduced a novel time-obfuscating technique that issues multiple user queries at different times to confuse the LBS. By sending a query randomly from a set of random trajectories based on the user's location, the LBS cannot know the user's real trajectory. Terrovitis and Mamoulis [84] considered spatiotemporal obfuscation to protect the published trajectories of users. A similar idea was presented by Ghinita *et al.* [85] in their spatiotemporal cloaking approach.

There are some papers that consider more complex adversarial knowledge. Duckham and Kulik [86] used obfuscation graphs to apply the concept of location obfuscation to road networks. Ghinita *et al.* [85] considered background map knowledge represented by a set of privacy-sensitive features.

Xiao and Xiong [87] developed a framework to preserve location privacy that accounts for the temporal correlations in location data.

3) DIFFERENTIAL PRIVACY-BASED METHODS

The application of differential privacy to location protection has been investigated in several recent papers. The definition of geo-indistinguishability [27] formalizes the notion of protecting a user's location within a radius r with a level of privacy that depends on r. The level of privacy is achieved by adding controlled random noise to the user's location. Bordenabe *et al.* [88] showed that, given a desired degree of geo-indistinguishability, it is possible to construct a mechanism that minimizes service quality loss using linear programming techniques.

However, Kifer and Machanavajjhala [89] showed that differential privacy will only erase the evidence of a single individual's private value when the individuals in the data are independent. This means there is potential for privacy leaks when the individuals' private values are correlated, as discussed by Olteanu *et al.* [90].

Generally speaking, obfuscation schemes will sacrifice the user's utility. While there is always a tradeoff between utility and privacy, there are some special cases. For example, Soma *et al.* [91] investigated location privacy protection in trip planning (TP) queries. They designed a method to protect location privacy by sending a false or cloaked location to the service provider that still yielded exact results for the TP queries. In this case, obfuscation is a good choice for privacy protection as there is no performance degradation.

D. REDUCING LOCATION INFORMATION SHARING

1) CACHING

Cache systems have been proposed as a way to improve user privacy. In these systems, the POI data is prefetched and stored in cache before arriving at an area [92]. However, this means a huge amount of service data needs to be stored. MobiCrowd [93] preserves user privacy by querying neighbors for service data before sending the query to the LBS server but, if neighboring users cannot provide the answers, the query is sent to the LBS server and is still at risk. Zhu *et al.* [94] proposed the Mobicache scheme which attempts to cache additional data that has not yet been cached.

TABLE 2. Comparison of location privacy preservation mechanisms by adversary and attack models.

Location Privacy Preservation Mechanism		Adversary and Attack			
		Information Obtain*	Knowledge£	Attack Method $	Target
Cryptography-based	PIR [8]	Col./Eav.	Obs./Con.	Con./Pro.	Identity/Position
Anonymization	k-anonymity [10]	Col./Eav.	Observed	NC†	Identity (non-consistent)
	Distributed k-anonymity [55] [57]	Col./Eav./Com.	Obs./Con.	Con./Collusion	Identity (non-consistent)
	l-diversity [59]	Collecting	Obs./Con.	Context linking	Identity (non-consistent)
	Historical k-anonymity [61]	Collecting	Obs./Con.	Context linking	Identity (consistent)
	Mix-zone [9]	Collecting	Obs./Con.	Context linking	Identity (consistent)
	Mix-zone with road networks [64] [62]	Collecting	Obs./Con.	Context linking	Identity (consistent)
	Trajectory mix-zone [65]	Collecting	Obs./Con.	Context linking	Identity (consistent)
Obfuscation	Dummy locations [11]	Collecting	Observed	NC	Position
	Realistic dummies [76] [78] [79]	Collecting	Obs./Con.	Context linking	Position
	Dummy trajectories [74]	Collecting	Obs./Con.	Context linking	Position/Time
	Spatial obfuscation [12]	Collecting	Observed	Context linking	Position
	Obfuscation to road networks [86]	Collecting	Obs./Con.	Context linking	Position
	Obfuscation to correlated locations [87]	Collecting	Obs./Con.	Con./Pro.	Position
	Time obfuscation [83]	Collecting	Observed	Context linking	Time
	Spatiotemporal obfuscation [84]	Collecting	Obs./Con.	Context linking	Position/Time
	Geo-indistinguishable [27]	Collecting	Observed	Probability	Position
Reducing location sharing	Caching [13] [95]	Col./Eav./Com.	Obs./Pre./Con.	NC	Identity/Position/Time
	Game theory [28]	Col./Eav./Com.	Obs./Pre./Con.	NC	Identity/Position/Time

† NC: Not specified.
* Col. : Collecting; Eav. : Eavesdropping; Com.: Compromising.
$ Con. : Context linking; Pro. : Probability; Col.: Collusion.
£ Obs. : Observed; Con. : Context; Pre.: Precise.

However, it does not consider side information, which may be used by an adversary to infer the real location of users. Niu *et al*. [13] proposed a privacy metric to model the effect of caching. Their cache-aware dummy selection algorithms carefully combine k-anonymity, caching, and side information to achieve a higher privacy degree and caching hit ratio. But cooperation among community members is still required. Liu *et al*. [95] proposed a framework that enhances the privacy of LBS in wireless vehicular network scenarios through active caching.

2) GAME THEORY

Alternatively, a game theory approach can be used to reduce location information sharing. For example, Liu *et al*. [28] proposed a framework that enhances the location privacy of MCS applications by reducing the bidding and assignment steps in the MCS cycle.

E. COMPARISONS AND DISCUSSIONS

1) LPPMS VS. OTHER PRIVACY-PRESERVATION TECHNIQUES

Just as location privacy is a subcategory of data privacy, LPPM is a subcategory of privacy preservation techniques. On the one hand, the ideas behind most LPPMs are derived from generic privacy protection techniques. For example, obfuscation can be used to disguise other types of data, such as figures, and cryptography can be applied to any information. But, on the other hand, most LPPMs need to be modified to suit the particular characteristics of location data. A typical example is the notion of geo-indistinguishability [27], which associates a level of privacy with a radius r from the user's location according to a generic differential privacy definition. Additionally, special attention needs to be paid to the ability of location data to reveal connections between different information as stated in Subsection II-D. In fact, a context linking attack is one of the most important research issues for many existing LPPMs, as can be seen in Table 2.

2) COMPARISONS OF THE FOUR DIFFERENT GROUPS

Consider an application that finds nearby POIs to compare the four types of LPPMs. As shown in Fig. 5, there are four users - Alice, Bob, Chuck, and Eve - who use an LBS to find nearby locations. Cryptography-based mechanisms encrypt all the information (see Fig. 5(a)). Anonymization schemes remove the true user identities, replacing them with {u1, u2, u3, u4} (see Fig. 5(b)). Obfuscation methods extend the precise user locations to a range of possible locations (see Fig. 5(c)). Finally, since Alice and Bob are close to each other, and they are both looking for a restaurant, they can share information, reducing the number of queries sent to the LBS server by one query (see Fig. 5(e)).

From the above example, it is clear that LPPMs are differentiated by their basic ideas. Cryptography schemes lower the risk of an adversary obtaining information. Anonymization breaks the links between identities and locations to make the information worthless. Obfuscation blurs the information to reduce the risk of disclosure. And reducing the amount of location sharing reduces the amount of information generated and transmitted through the whole system.

Additionally, each approach considers different types of adversaries and the attacks they perpetrate. Obfuscation schemes focus on spatial and temporal information, whereas anonymization emphasizes identity protection. While cryptography and reducing location sharing protect all three attributes of location information. An overall comparison is listed in Table 2.

Finally, anonymization schemes differ from the three other groups in two further ways. First, the anonymization is

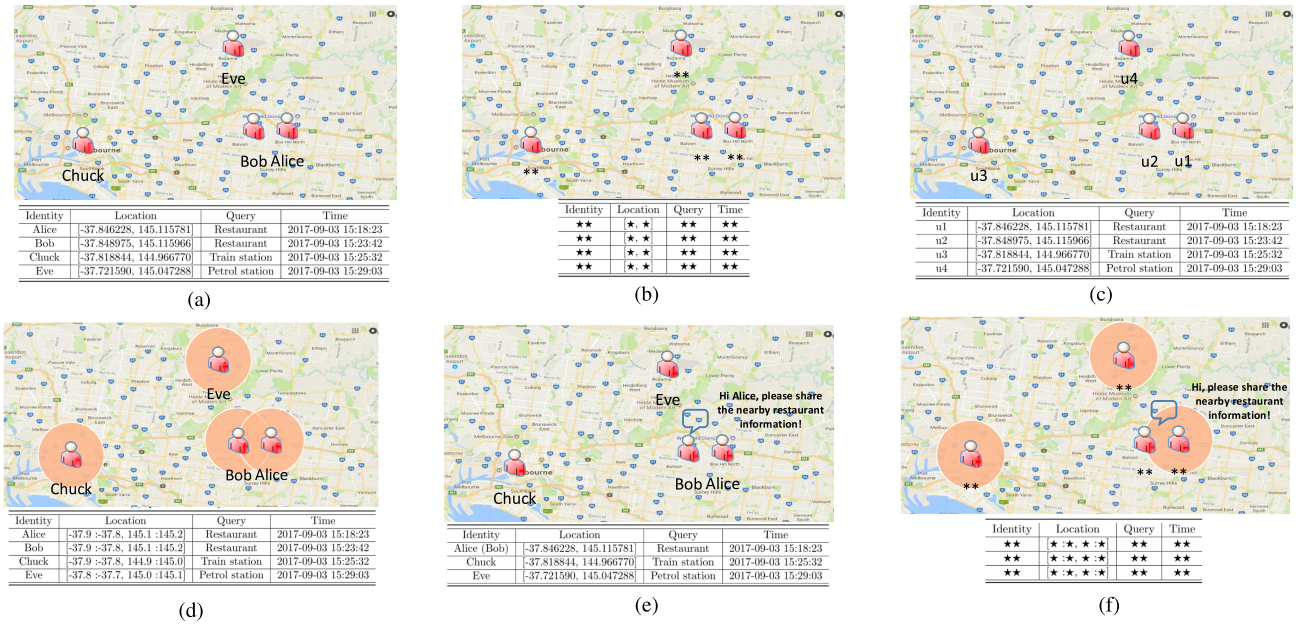


FIGURE 5. Comparison of different LPPMs using a POI finder as an example. (a) Queries without privacy protection. (b) Queries with encryption. (c) Queries with anonymization. (d) Queries with obfuscation. (e) Reducing unnecessary queries. (f) Queries with multiple privacy protection schemes.

TABLE 3. Comparison of location privacy preservation mechanisms by TTP and metrics.

Location Privacy Preservation Mechanism		TTP required	Location Privacy Metric
Cryptography-based	PIR [8]	No	Certainty
Anonymization	Mix-zone [9]	Yes	Certainty
	k-anonymity [10]	Yes	Certainty
Obfuscation	Dummy locations [11]	No	Correctness
	Spatial obfuscation [12]	No	Correctness
	Temporal obfuscation [83]	No	Correctness
	Spatiotemporal obfuscation [85]	No	Correctness
	Geo-indistinguishable [27]	No	Geo-Indistinguishability
Reducing location sharing	Caching [13]	No	Information gain or loss
	Game theory [28]	No	Information gain or loss

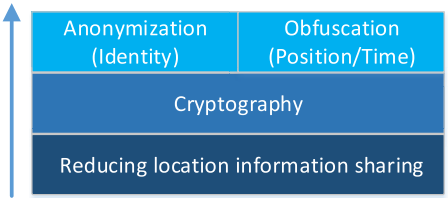


FIGURE 6. Different LPPMs can be used at the same time.

usually entrusted to a third party, as shown in Table 3. Second, these approaches require user cooperation to achieve their goals.

Despite these differences among the LPPMs, it is important to emphasize that they are not mutually exclusive. As shown in Fig. 6, it is common to combine different techniques by first trying to reduce any unnecessary information sharing, and then protecting the remaining transmissions with encryption. Anonymization is often used to protect identity information, and obfuscation is used to protect position/time information. Fig. 5(f) illustrates an example where multiple schemes have been adopted at the same time.

3) EVOLUTION OF METHODS WITHIN EACH GROUP

It is also interesting to look at the evolution of the methods within each group. The original version of a method is generally based on simple adversary models and assumptions. Then, new methods consider more complicated cases and expand to include more contextual knowledge or more comprehensive targets. Take anonymization schemes as an example. As shown in Fig. 7, anonymization was divided into two groups from the outset. One group was based on the idea of hiding a user among other similar anonymous users, i.e., k-anonymity; another group was based on changing the identities within the set; i.e., mix-zones. Each group was then further improved by more complicated information acquisition methods and knowledge of adversaries. Similarly, Fig. 8 shows the evolution of the different methods in the obfuscation group.

V. PERFORMANCE EVALUATION: LOCATION PRIVACY METRICS

Comparing the performance of different LPPMs is highly dependent on the ability to quantify location privacy.

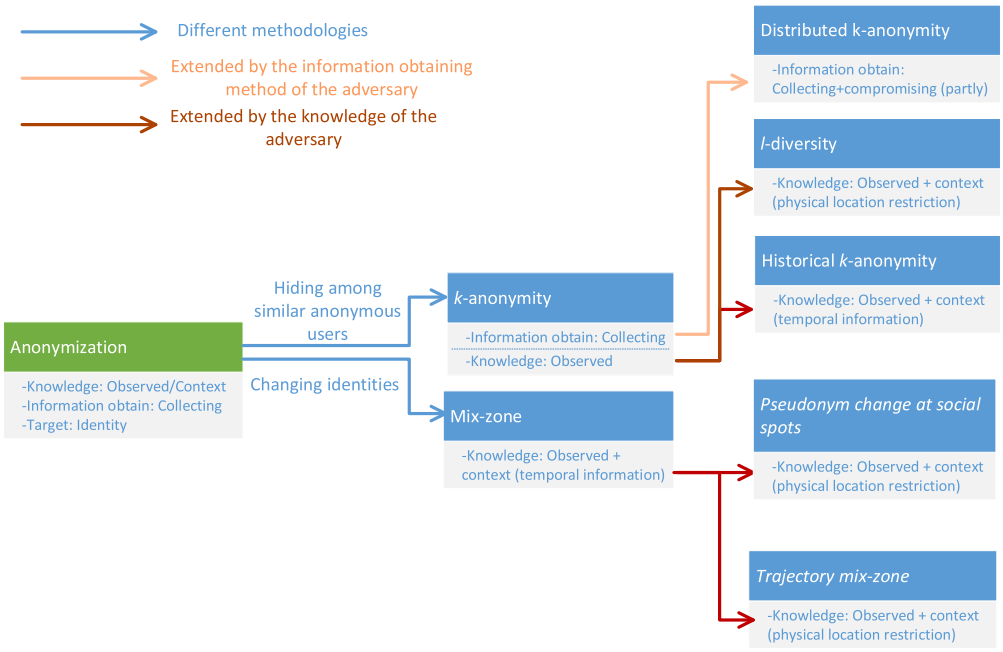


FIGURE 7. Evolution of location privacy methods using the anonymization scheme.

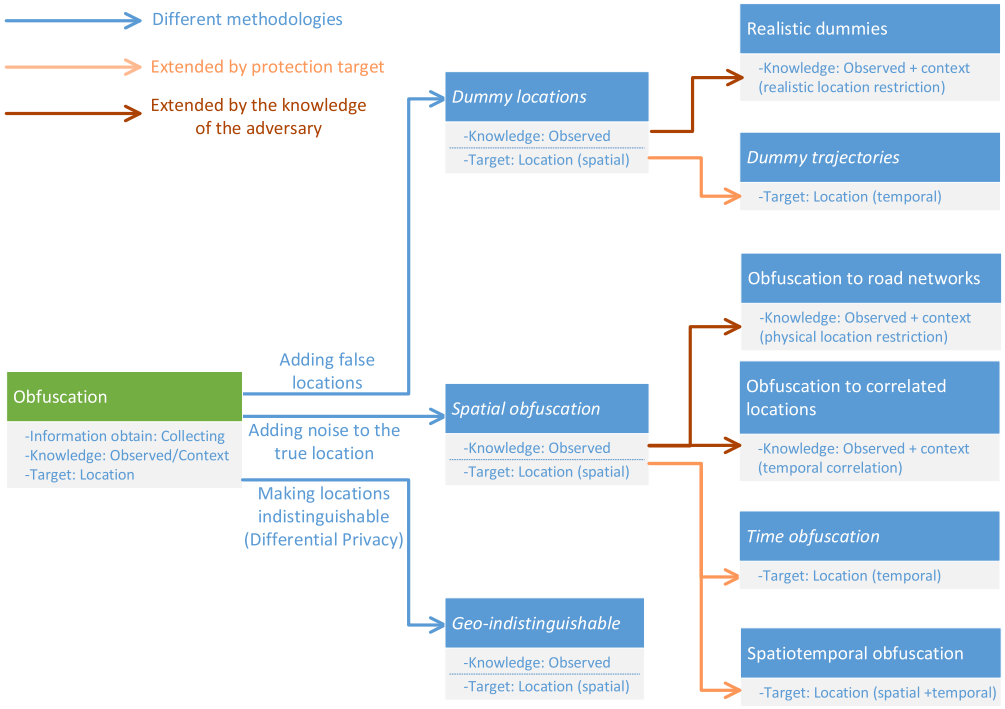


FIGURE 8. Evolution of location privacy methods using the obfuscation scheme.

However, there is not yet a standard for evaluating privacy. Indeed, it is rare for even two different research projects to use the same method of quantification [96].

Wagner and Eckhoff [97] provides a very detailed summary of privacy metrics, including many metrics that are not even in the scope of location privacy. Shokri *et al.* [26] argues that location privacy metrics should consider three key aspects: accuracy, uncertainty, and correctness. In this section, we reorganize the existing metrics into five categories.

A. CERTAINTY

Certainty or uncertainty metrics are used to measure the ambiguity of an adversary with respect to finding a unique answer. This answer could be an identity or any other spatial or temporal information about the location.

1) NUMERICAL METRICS

Duckham and Kulik [98] defines the ''level of privacy'' as the number of different location coordinates sent by a user with a single location-based query. More points mean more ambiguity and, hence, a higher privacy level. The goal of their system is to be as ambiguous as possible while still getting the right answer for a POI query.

In the k-anonymity group of LPPMs, k is used to represent the level of privacy [10]. Similarly, p is used in p-sensitivity [58], and l is used in l-diversity [59].

2) ENTROPY-BASED METRICS

Shannon entropy is the basis for many metrics. In location privacy, entropy-based metrics are computed based on the posterior probability of the adversary's estimates $\hat{x}$ based on his observations o:

$$\sum_{\hat{x}} Pr(\hat{x}|o) \log \frac{1}{Pr(\hat{x}|o)}. \tag{1}$$

Actually, numerical metrics can easily be converted into entropy-based metrics. For example, in a k-anonymity system, the equivalent entropy is

$$\sum_{k} \frac{1}{k} \log \frac{1}{1/k}. \tag{2}$$

The resulting value can be used to measure how well an adversary can identify a specific user in an anonymity set and disclose their position.

Entropy has also been used in cases where privacy is measured at more than one point in time. For example, in scenarios where an the adversary tracks users over a period of time, entropy is computed at every point in time and the underlying probabilities are updated after each timestamp using Bayesian belief tables [99]. This approach accounts for the prior knowledge that the adversary acquired during previous timestamps once the first timestamp has been calculated.

The disadvantage of certainty metrics is that they do not take the correctness of the adversary's estimates into account because the true position x is not considered in the equation. This might be problematic. For example, if two positions are very close to each other, the locations may be revealed despite high entropy [100].

B. CORRECTNESS

1) ADVERSARIAL SUCCESS RATES

This metric measures the probability that an adversary will be successful, or the percentage of successes in a large number of attempts. Depending on the application scenario, success can be defined in different ways. For example, to evaluate the performance of an inference attack, Li *et al.*'s [30] successful rate is based on the success of inferring the correct demographics.

2) DISTANCE-BASED METRICS

Distance-based metrics quantify the error or expected distance between the true information and the estimated information, using any distance metric $d()$. A distance metric for a single location can be computed by the posterior probability of the adversary's estimate $\hat{x}$ based on their observations o, while the true position is x:

$$\sum_{\hat{x}} Pr(\hat{x}|o) d(x, \hat{x}). \tag{3}$$

And this can be extended to a trajectory by summation over multiple timestamps [100].

C. INFORMATION GAIN OR LOSS

Information gain or loss metrics measure the amount of information that an adversary can possibly gain. They assume that privacy is higher when an adversary can gain less information. Similar to uncertainty metrics, many information gain metrics found their roots in numerical metrics or entropy-based metrics.

For example, Liu *et al.* [95] defines the ''Privacy degree'' as the percentage of queries that cached content can respond to as opposed to the service provider. As the cached content is in local memory, it is more secure than the LBS server.

Similarly, the number of packages uploaded by participants in MCS applications can also be used to measure privacy levels [28].

D. GEO-INDISTINGUISHABILITY

In statistical databases, differential privacy guarantees that any disclosure is equally likely regardless of whether or not an item is in the database [101]. In the context of location privacy, Andrés *et al.* [27] proposed a useful term ''Geo-indistinguishability'' to measure the level of privacy.

Definition 1 (***ϵ-Geo-indistinguishability):*** For each true location $x \in \mathcal{X}$, a mechanism $\mathcal{K}$ is a probabilistic function assigned to x as a probability distribution of $\mathcal{Z}$. And $Pr(\mathcal{K}(x) = z), z \in \mathcal{Z}$ is the probability that z is the location generated by $\mathcal{K}$ from x. Then the *Geo-indistinguishable level* of $\mathcal{K}$ is defined as:

$$\begin{aligned} GIL(\mathcal{K}, x, x') &= \sup_{z \in \mathcal{Z}} \left| \ln \frac{Pr(\mathcal{K}(x) = z)}{Pr(\mathcal{K}(x') = z)} \right| \\ &= \sup_{z \in \mathcal{Z}} \left| \ln \frac{Pr(z|x)}{Pr(z|x')} \right|, \end{aligned} \tag{4}$$

where we use $Pr(z|x)$ instead of $Pr(\mathcal{K}(x) = z)$ for simplicity.

We say $\mathcal{K}$ satisfies ϵ-Geo-indistinguishability if and only if, for all $x, x' \in \mathcal{X}$ and $z \in \mathcal{Z}$:

$$GIL(\mathcal{K}, x, x') \leq \epsilon d_2(x, x'), \tag{5}$$

where $d_2(x, x')$ is the Euclidean distance between locations. Note that for all points x' within a radius of r from x, the definition forces the corresponding probabilities of generating the same released location z to be ϵr distant at most.

Therefore, the parameter ϵ represents the level of Geo-indistinguishability.

E. TIME

Time-based metrics focus on time as a resource that an adversary needs to spend to compromise a user's privacy. In some location privacy issues, the adversary aims to not only break privacy at a single time point, but also to track a target's location over time. For example, the adversary's tracking ability is measured by the maximum tracking time in [102], which is defined as the cumulative time that the size of the target's anonymity set remains 1.

This metric tends to overestimate a target's privacy because it assumes that the adversary has to be completely certain. To avoid the overestimation of privacy, the mean time to confusion measures the time during which the adversary's uncertainty stays below a confusion threshold [103].

F. PERFORMANCE EVALUATION

In this subsection, we compare the performance of several LPPM mechanisms in a POI-finding scenario. Of the five metrics discussed above, ***correctness*** is the one which can be used to evaluate the most methods.

Consider a tradeoff with respect to the service quality loss (SQL) metric discussed in [104]. SQL is defined as the expected distance between the reported (observed) location o and the user's true location x:

$$\sum_{x} Pr(o|x)d(x, o). \tag{6}$$

The mechanisms compared here are:

1) k-anonymity [10] with some minor changes to the original version for ease of comparison with the other two. When a user wants to query POI information, instead of sending their true location, they randomly select one location from the k-anonymity group.
2) Classic spatial obfuscation [12], which sends a circular area with radius of R to the LBS server instead of the precise user position.
3) Geo-indistinguishability [27] with a planar Laplace distribution to generate the noise that is added to the precise locations.

In all cases, the area of interest is assumed to be a two-dimensional plane, the users' real locations are randomly generated throughout the region. No contextual information is considered.

First, we set the parameters of each mechanism in such a way that the SQL is the same for all and compare the correctness of each. Fig. 9(a) shows that the geo-indistinguishable mechanism offers the best performance. among the mechanisms. (A greater value of correctness means that it is hard for the adversary to obtain the correct location.) k-anonymity and obfuscation provided a similar performance with our settings. Once the values of correctness were fixed, the geo-indistinguishable mechanism introduced the smallest SQL, as shown in Fig. 9(b).

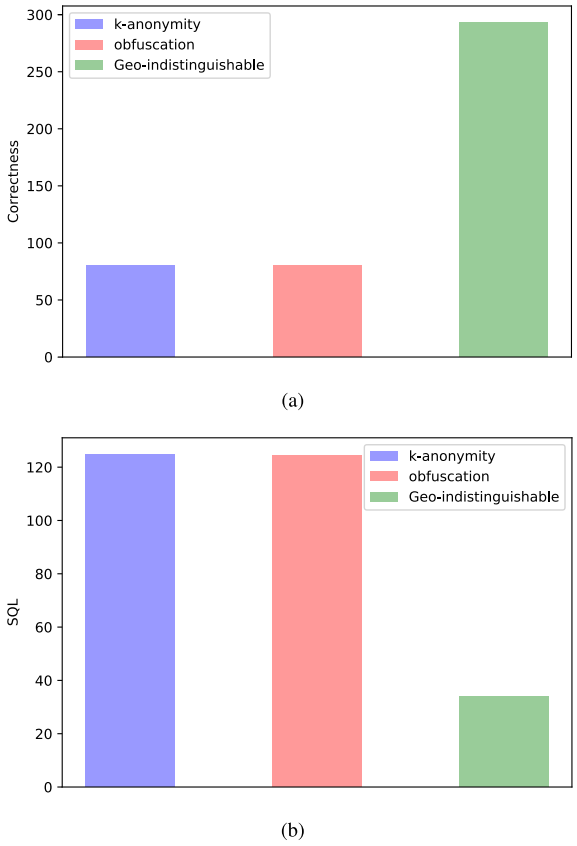


FIGURE 9. Performance comparison of different LPPMs by simulation. (a) SQL = 100. (a) Correctness = 100.

G. DISCUSSION ON PERFORMANCE METRICS

The metrics discussed above are the most frequently used in current research endeavors. However, there are some other ones. For instance, Shokri *et al.* [26] mentions an ***accuracy*** metric, which is used to quantify the accuracy of the adversary's estimation. However, this metric it is not used very often as it does not reflect the certainty or the correctness of the results.

Although we used the correctness metric for our comparison, it is important to emphasize that different groups of LPPMs should use different metrics as they have different protection targets and methodologies. As such, evaluating the differences between LPPMs without considering specific contexts and goals is a relatively arbitrary exercise. Table 3 summarizes the most commonly-used metrics for a selection of LPPMs for the interest of readers.

VI. LOCATION PRIVACY IN PRACTICAL APPLICATIONS

Having discussed the different aspects of location privacy issues in LBSs, in this section, we investigate the current status of location privacy in practical terms.

A. LOCATION-BASED SERVICES IN PRACTICAL APPLICATIONS

LBSs experienced a boom along with the emergence of the smartphone and are currently widely used in a variety of contexts, such as health, entertainment, work, and personal

TABLE 4. Summary of location information types in the current LBS applications.

LBS Name		Identity Information	Spatial Information	Temporal Information
Geo-social Services	Check-in	Consistent	Single, Direct	Non-real-time
	Geo-tagged posters	Consistent	Single, Direct	Real-time
	Finding nearby friends	Consistent	Single, Indirect	Real-time
Geo-information Services	Navigation	Non-consistent	Single, Trajectory, Direct	Real-time
	Finding POI	Non-consistent	Single, Trajectory, Direct, Indirect	Real-time, Non-real-time
Sports and health assistant	Sports tracking	Consistent	Trajectory, Direct	Real-time
Augmented reality (AR) games	Pokemon Go	Consistent	Trajectory, Indirect	Real-time

TABLE 5. Summary of LBSs provided by different LBAs.

LBA Name	Check-in	Geo-tagged posters	Finding nearby friends	Navigation	Finding POI	Sports tracking	AR Game
Foursquare/Swarm	✓		✓		✓		
Facebook	✓		✓		✓		
Twitter		✓					
Google Maps				✓	✓		
Wechat		✓	✓				
Pokemon Go							✓
Fitbit						✓	
Yelp	✓				✓		

life. According to the different application scenarios, current LBSs can be grouped into the following categories [105]:

- Geo-social services [106]: These services have introduced location information into social networking platforms to enrich interactivity and the relationships between people. The very first service of this kind was the check-in service. Foursquare [107] was one of the earliest LBS applications to provide a check-in function. Glympse is a similar application, and there are many others [108]. This simple check-in concept was soon extended to encompass a broader vision of geo-social services, including location sharing among friends (Foursquare), posting geo-tagged tweets (Twitter [109]) or moments (Wechat), and to finding nearby friends (Wechat, Facebook).
- Information services: Current navigation systems provide real-time traffic condition reports and route selection based on a user's location. Passengers can obtain public transport timetables at bus stops and train stations. Additionally, some services provide nearby-POI information to their users. Yelp [110] was one of the first online local POI search services. Its mobile version provides an easy way for users to find nearby POIs by allowing Yelp to access to their current location. Similarly, many other traditional web-based services, such as Tripadvisor [5], have LBS versions for mobile platforms. In addition, unmanned autonomous systems, or autonomous systems for short, are becoming mainstream in practice, with the widespread introduction of autonomous vehicles, drones, and so on. These systems also include LBSs.
- Healthcare assistant systems: Fitbit [6] is an example of this type of LBS, which is an activity tracker and a wireless-enabled wearable technology device that measures data, such as the number of steps walked, heart rate, quality of sleep, steps climbed, and other personal metrics involved in fitness.
- Augmented reality (AR) games: While the craze has cooled somewhat, Pokemon Go [7] has launched a new era of AR games by combining the addictive creature collection and monster battling play in Nintendo's Pokemon with Niantic's augmented reality technology. Players explore their neighborhood on foot, using their smartphone as a map and viewfinder to discover and collect Pokemon. Pokemon, and their accoutrements, can also be collected from Pokestops - shops and gyms tied to real-world locations that you need to physically travel to - which encourages players to explore their neighborhood and get their feet in gear.

The above summary of categories is based on the functions and aims of the services, but different LBSs use different types of location information as well. Table 4 lists the types of location information used in the different LBSs.

The current trend is to integrate multiple functions into one application. For example, the original Foursquare has become a location-aware smart-search tool that focuses on discovering nearby locations, events, restaurants, and shops, while Swarm caters to those addicted to checking in and location sharing with friends. Google Maps has paired its navigation system with location awareness functions that allow you to easily find everything you need, like nearby POIs, traffic, and the estimated travel time to any destination.

To distinguish the application from the provided service, we have used the term location-based application (LBA) to refer to any device, software, or mobile app that provides an LBS. Given that one LBA can house multiple LBSs, the types of LBSs provided in popular LBAs have been provided in Table 5) as general context.

B. HOW DO PEOPLE CARE ABOUT THEIR LOCATION PRIVACY?

People's views on location privacy changes over time. Studies prior to 2010 [111] [112] [113] show that the general public

were not very concerned about their location privacy. However, with the boom of LBSs in recent years, new research has been conducted that tells a different story.

Below, we summarize these opinions in two different respects.

1) DO PEOPLE REALLY KNOW HOW MUCH OF THEIR LOCATION INFORMATION HAS BEEN COLLECTED OR REVEALED?

Some researchers argue that people do not much care about their location privacy because they are often unaware of the amount and frequency of the data collected by their applications. Aalmuhimedi *et al*. [114] show that a user's location can be shared more than 5000 times in a two-week period. And participants in the study knew how frequently their data was being collected, 95% of them reassessed their permissions, and 58% further restricted some of their permissions.

2) HOW DO PEOPLE CARE ABOUT THEIR LOCATION PRIVACY?

Fawaz and Shin [115] surveyed 180 smartphone users. 78% of the participants believe that apps accessing their location can pose privacy threats. Also, 85% of them reported that they care about who accesses their location information. 77% of the users included the term ''privacy'' as a factor affecting their choice in installing a privacy protection mechanism.

Thus, we cannot arbitrarily assert that people care or do not care about their location privacy nowadays. In most cases, people are weighing the price of information sharing with the corresponding benefits. As people become more aware of the risk of disclosing their location information, it is reasonable to believe that the majority of the public will pay more attention to location privacy issues.

C. HOW TO HELP USERS SELECT AN LPPM

The research in LPPMs provide powerful tools for users to protect their privacy. However, the reality of location privacy issues are still far from satisfactory for several reasons. First, users are not generally very sure about the LPPMs used in certain applications. Additionally, it is difficult for the average person to understand the advantages and consequences of using LPPMs. Lastly, as privacy is always a tradeoff between its benefits and its risks, different users may have different views about privacy issues. Therefore, users need guidance to help them select the most appropriate LPPM for their own personal circumstances.

Most LBSs have a default configuration that users can modify as desired. But customizing these settings requires effort, and users often accept the default rather than modifying these preferences to meet their needs [116]. Thus, the default settings can have a large impact on the resulting privacy for users. Organizations and developers that create applications must make decisions about default privacy configurations, and sometimes those decisions do not fully meet the user's privacy needs [117].

A variety of research has examined how to automatically determine or recommend personalized privacy settings.

1) MODEL-BASED METHODS

One strand of research classifies or score a user's attitudes toward privacy by asking users to answer a series of questions about privacy, and then setting privacy levels accordingly [118]. Liu and Terzi [119] framework for computing privacy scores using profile item sensitivity and the user's social network level. Minkus and Memon [120] examined characterizing privacy settings into a single score that can be used to aid users when configuring a privacy policy or comparing two given policies. This approach includes both naive and weighted methods, which take sensitivity and visibility into account. Watson *et al*. [121] computes a score to characterize a user's privacy preferences without assumptions about how each piece of data should impact the score.

2) LEARNING-BASED METHODS

Others have examined using machine learning algorithms and other algorithms to automatically determine settings based on a user's previous settings or behaviors [122]. For example, Sinha *et al*. [123] gathers information about users' previous Facebook posts to predict better default policies for future posts. Similarly, Shehab and Touati [124] and Bilogrevic *et al*. [125] suggest using machine learning to automatically configure complex privacy settings for friends based on the configurations for a selected set of friends.

D. EXAMPLES OF LOCATION PRIVACY PRESERVATION SCHEMES IN PRACTICAL APPLICATIONS

Despite the numerous research proposals for location privacy protection from various angles and in various scenarios, the majority have not found their way into common use. Existing mechanisms suffer several shortcomings that hinder their deployment in the real world. These shortcomings can be described in terms of effectiveness, efficiency, and practicality. For example, cryptographic methods face the problem of inefficiency due to high computational costs. And most of the proposed mechanisms rely on unrealistic assumptions, making real-world deployment difficult [115].

Encouragingly, more and more LBS providers are beginning to emphasize privacy issues and are introducing countermeasures into their applications. For example, Twitter [109] has enabled users to select the location accuracy of the geotagged posters. Glympse [108] enables users to share locations that will automatically expire, so the locations are never permanently posted. SocialRadar [126] provides an overview of what is going on with the people in your social network and who is around, but users can choose to be anonymous or invisible when using the app. For people who wish to remain anonymous, Yik Yak [127] is a fun location-based sharing app that removes the pressure to have your identity strapped to a profile. This app shows you a stream of short anonymous posts from people around your geographic area. When you post, you do have the option to show your exact location and

add a nickname but, otherwise, everyone is totally nameless in the community.

E. DISCUSSION ON PRIVACY IN APPLICATIONS

Overall, protecting the privacy of location data in real life still has a long way to go because the majority of people do not yet fully understand the power of location data, and the majority of businesses need to know more about location data management. The rapid development of LBSs has meant location ecosystems and location data are becoming more and more complicated. Yet, existing policies and the legal environment is not aligned with the current state of the technology. With the efforts from both academia and industry, we believe the situation will soon improve.

VII. FUTURE DIRECTIONS

A. LOCATION PRIVACY PROTECTION UNDER CORRELATIONS

Although the location privacy issues have been widely studied, most previous studies have focused on independent data, which assumes that all data were independently sampled from a universe. Despite this, a real-world dataset often exhibits strong coupling relations, where some records are frequently correlated with each other, and this may disclose more information than expected. Some research is beginning to account for the temporal and spatial correlations in location data [90] [128] [129], but these efforts are far from mature.

A further challenge is the correlation between location data and other databases. For example, health and medical records may be associated with people's location information to launch attacks. This is an important direction of research but has not yet been well-studied.

B. LOCATION PRIVACY IN BIG DATA AND DEEP LEARNING ERA

The massive amounts of data available on the Internet and the unprecedented accuracy of deep learning methods are continually reshaping many areas of research and industry. At the same time, these methods present obvious privacy issues [130]. For example, current deep learning-based methods can detect type of objects [131], and recognize celebrities and landmarks from personal photos posted on social networks. These methods can automatically collect and process millions of photos or videos to reveal private information. For example, Weyand *et al*. [46] were able to predict the geolocations of users with high accuracy just from their personal photos.

Traditional privacy preservation methods seem powerless when faced with large-scale deep learning tools and a Big Data training set. Hence, location privacy problems need to be reinvestigated in a Big Data and deep learning context.

VIII. CONCLUSIONS

This study surveys the literature on location privacy and combines it into a unified framework. The existing research on this topic, especially in recent years, has covered almost every aspect of location privacy. By classifying each aspect of this research and identifying the connections between studies, we can draw several conclusions as follows.

- The definition of location privacy provided in this paper includes the three aspects of privacy that are important to users: identity, spatial information (position), and temporal information (time) and can, therefore, be used as a generic definition for location privacy within the field. The importance of location data is high due to its ability to link disparate datasets and provide a much more complete profile of an individual or organization. In addition, location data has unique characteristics including the massive scale of available location information, its high correlations, and its dynamic and unequal importance.
- A variety of adversarial features and attacks have been explored in the literature. Machine learning/deep learning represents an emerging threat and has recently been used as an attack method based on large-scale location data mining.
- Among the four groups of location privacy preservation schemes studied in this paper, obfuscation and anonymization mechanisms are the most predominant. Cryptographic mechanism are a classic technique but these methods have not seen much improvement for a while. The idea of reducing the amount location information that is shared has emerged recently, and this technique can be combined with any and all of the other methods. Different groups of LPPMs use different evaluation metrics, as they have different protection targets and methodologies. Moreover, improvements to LPPMs tend to concern the more and more realistic contexts for attacks and adversaries.
- Privacy preservation in practical applications is still in its preliminary stages. Only a few basic LBAs incorporate simple obfuscation and anonymization methods.

We believe that this study will shed light on the research issues associated with location privacy and will promote the advancement and development of future location privacy applications. With the increasing attention paid to the importance of location privacy, we expect to see more research and its application in this area.

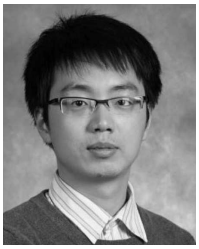
REFERENCES

[1] *U.S. Location-Based Service Users*. Accessed: Dec. 19, 2016. [Online]. Available: https://www.statista.com/statistics/436071/location-based-service-users-usa/
[2] *Facebook*. Accessed: Dec. 19, 2016. [Online]. Available: https://www.facebook.com/
[3] *Wechat*. Accessed: Dec. 19, 2016. [Online]. Available: https://www.wechat.com
[4] *Google Maps*. Accessed: Dec. 19, 2016. [Online]. Available: https://www.google.com.au/maps
[5] *Tripadvisor*. Accessed: Jan. 1, 2016. [Online]. Available: https://www.yelp.com.au/
[6] *Fitbit*. Accessed: Dec. 19, 2016. [Online]. Available: https://www.fitbit.com
[7] *Pokemon Go*. Accessed: Dec. 19, 2016. [Online]. Available: http://www.pokemongo.com/
[8] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private queries in location based services: Anonymizers are not necessary," in *Proc. ACM SIGMOD*, 2008, pp. 121–132.

[9] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive Comput.*, vol. 2, no. 1, pp. 46–55, Jan. 2003.
[10] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *Proc. ACM MobiSys*, 2003, pp. 31–42.
[11] H. Kido, Y. Yanagisawa, and T. Satoh, "An anonymous communication technique using dummies for location-based services," in *Proc. IEEE ICPS*, Jul. 2005, pp. 88–97.
[12] C. A. Ardagna, M. Cremonini, S. D. C. di Vimercati, and P. Samarati, "An obfuscation-based approach for protecting location privacy," *IEEE Trans. Depend. Sec. Comput.*, vol. 8, no. 1, pp. 13–27, Jan./Feb. 2011.
[13] B. Niu, Q. Li, X. Zhu, G. Cao, and H. Li, "Enhancing privacy through caching in location-based services," in *Proc. IEEE INFOCOM*, Apr./May 2015, pp. 1017–1025.
[14] J. Krumm, "A survey of computational location privacy," *Pers. Ubiquitous Comput.*, vol. 13, no. 6, pp. 391–399, 2009.
[15] M. Decker, "Location privacy—An overview," in *Proc. 7th Int. Conf. Mobile Bus.*, Jul. 2008, pp. 221–230.
[16] M. Duckham, "Moving forward: Location privacy and location awareness," in *Proc. ACM SIGSPATIAL Int. Workshop Secur. Privacy GIS LBS*, 2010, pp. 1–3.
[17] A. Khoshgozaran and C. Shahabi, "A taxonomy of approaches to preserve location privacy in location-based services," *Int. J. Comput. Sci. Eng.*, vol. 5, no. 2, pp. 86–96, Nov. 2010.
[18] A. Solanas, J. Domingo-Ferrer, and A. Martínez-Ballesté, "Location privacy in location-based services: Beyond TTP-based schemes," in *Proc. ACM Int. Workshop Privacy Location-Based Appl. (PILBA)*, 2008, pp. 12–23.
[19] M. Wernke, P. Skvortsov, F. Dürr, and K. Rothermel, "A classification of location privacy attacks and approaches," *Pers. Ubiquitous Comput.*, vol. 18, no. 1, pp. 163–175, Jan. 2014.
[20] S. Oya, C. Troncoso, and F. Pérez-González, "Back to the drawing board: Revisiting the design of optimal location privacy-preserving mechanisms," in *Proc. ACM CCS*, 2017, pp. 1959–1972.
[21] M. Conti, J. Willemsen, and B. Crispo, "Providing source location privacy in wireless sensor networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 3, pp. 1238–1280, 3rd Quart., 2013.
[22] M. Grissa, B. Hamdaoui, and A. A. Yavuza, "Location privacy in cognitive radio networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1726–1760, 3rd Quart., 2017.
[23] J. D. Roth, M. Tummala, J. C. McEachen, and J. W. Scrofani, "On location privacy in LTE networks," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 6, pp. 1358–1368, Jun. 2017.
[24] M. Grissa, A. A. Yavuz, and B. Hamdaoui, "Preserving the location privacy of secondary users in cooperative spectrum sensing," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 2, pp. 418–431, Feb. 2017.
[25] R. Shokri, J. Freudiger, and J.-P. Hubaux, "A unified framework for location privacy," LCA, EPFL, Lausanne, Switzerland, Tech. Rep. EPFL-REPORT-148708, Jul. 2010.
[26] R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P. Hubaux, "Quantifying location privacy," in *Proc. IEEE Symp. Secur. Privacy*, 2011, pp. 247–262.
[27] M. E. Andrés, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Geo-indistinguishability: Differential privacy for location-based systems," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2013, pp. 901–914.
[28] B. Liu, W. Zhou, T. Zhu, H. Zhou, and X. Lin, "Invisible hand: A privacy preserving mobile crowd sensing framework based on economic models," *IEEE Trans. Veh. Technol.*, vol. 66, no. 5, pp. 4410–4423, May 2017.
[29] R. Shokri, G. Theodorakopoulos, and C. Troncoso, "Privacy games along location traces: A game-theoretic framework for optimizing location privacy," *ACM Trans. Privacy Secur.*, vol. 19, no. 4, p. 11, Feb. 2017.
[30] H. Li, H. Zhu, S. Du, X. Liang, and X. Shen, "Privacy leakage of location sharing in mobile social networks: Attacks and defense," *IEEE Trans. Depend. Sec. Comput.*, to be published.
[31] K. Barker *et al.*, "A data privacy taxonomy," in *Proc. Brit. Nat. Conf. Databases*, 2009, pp. 42–54.
[32] C.-Y. Chow and M. F. Mokbel, "Privacy of spatial trajectories," in *Computing With Spatial Trajectories*. New York, NY, USA: Springer, 2011, pp. 109–141.
[33] A. J. Blumberg and P. Eckersley, "On locational privacy, and how to avoid losing it forever," *Electron. Frontier Found.*, vol. 10, no. 11, pp. 1–7, 2009.
[34] *Why Location Privacy is Important*. Accessed: Nov. 30, 2016. [Online]. Available: http://www.itworld.com/article/2752981/mobile/why-location-privacy-is-important.html
[35] J. Krumm, "Inference attacks on location tracks," in *Proc. IEEE PERCOM*, May 2007, pp. 127–143.
[36] Y. Gu, Y. Yao, W. Liu, and J. Song, "We know where you are: Home location identification in location-based social networks," in *Proc. ICCCN*, Aug. 2016, pp. 1–9.
[37] J. Mahmud, J. Nichols, and C. Drews, "Home location identification of Twitter users," *ACM Trans. Intell. Syst. Technol.*, vol. 5, no. 3, p. 47, 2014.
[38] *How Burglars Use Facebook to Target Vacationing Homeowners*. Accessed: Nov. 30, 2016. [Online]. Available: http://www.ibtimes.com/how-burglars-use-facebook-target-vacationing-homeowners-1341325
[39] J. Bellatti *et al.*, "Driving habits data: Location privacy implications and solutions," *IEEE Security Privacy*, vol. 15, no. 1, pp. 12–20, Jan./Feb. 2017.
[40] *Tracing a Stalker*. Accessed: Nov. 30, 2016. [Online]. Available: http://www.nbcnews.com/id/19253352/WDexmYVOLD4
[41] *Authorities: GPS System Used to Stalk Woman*. Accessed: Nov. 30, 2016. [Online]. Available: http://usatoday30.usatoday.com/tech/news/2002-12-30-gps-stalkerx.htm
[42] *Steven Brown Used GPS Devices and Private Detectives to Stalk His Estranged Partner*. Accessed: Nov. 30, 2016. [Online]. Available: http://www.dailyecho.co.uk/news/14920127.Stalker_used_GPS_devices_and_private_detectives_to_stalk_his_estranged_partner
[43] K. Minami and N. Borisov, "Protecting location privacy against inference attacks," in *Proc. ACM workshop Privacy Electron. Soc.*, 2010, pp. 123–126.
[44] S. Gambs, M.-O. Killijian, and M. N. del Prado Cortez, "De-anonymization attack on geolocated data," *J. Comput. Syst. Sci.*, vol. 80, no. 8, pp. 1597–1614, 2014.
[45] T. Murakami and H. Watanabe, "Localization attacks using matrix and tensor factorization," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 8, pp. 1647–1660, Aug. 2016.
[46] T. Weyand, I. Kostrikov, and J. Philbin, "PlaNet-photo geolocation with convolutional neural networks," in *Proc. Eur. Conf. Comput. Vis.*, 2016, pp. 37–55.
[47] M. Li *et al.*, "All your location are belong to us: breaking mobile social networks for automated user location tracking," in *Proc. ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2014, pp. 43–52.
[48] S. Mascetti *et al.*, "Privacy in geo-social networks: Proximity notification with untrusted service providers and curious buddies," *VLDB J.*, vol. 20, no. 4, pp. 541–566, 2011.
[49] G. F. Marias, C. Delakouridis, L. Kazatzopoulos, and P. Georgiadis, "Location privacy through secret sharing techniques," in *Proc. IEEE Int. Symp. World Wireless Mobile Multimedia Netw.*, Jun. 2005, pp. 614–620.
[50] P. Chen, Y. Lin, W. Zhang, X. Li, and S. Zhang, "Preserving location and content privacy for secure ranked queries in location based services," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, Aug. 2016, pp. 892–899.
[51] B. Gedik and L. Liu, "Location privacy in mobile systems: A personalized anonymization model," in *Proc. IEEE ICDCS*, Jun. 2005, pp. 620–629.
[52] T. Xu and Y. Cai, "Exploring historical location data for anonymity preservation in location-based services," in *Proc. IEEE INFOCOM*, Apr. 2008.
[53] Z. Huo, Y. Huang, and X. Meng, "History trajectory privacy-preserving through graph partition," in *Proc. ACM Workshop Mobile Location-Based Service*, 2011, pp. 71–78.
[54] C. Bettini, S. Mascetti, X. S. Wang, D. Freni, and S. Jajodia, "Anonymity and historical-anonymity in location-based services," in *Privacy in Location-Based Applications*. Berlin, Germany: Springer, 2009, pp. 1–30.
[55] G. Zhong and U. Hengartner, "A distributed k-anonymity protocol for location privacy," in *Proc. IEEE PerCom*, Mar. 2009, pp. 1–10.
[56] J. Li, H. Yan, Z. Liu, X. Chen, X. Huang, and D. S. Wong, "Location-sharing systems with enhanced privacy in mobile online social networks," *IEEE Syst. J.*, vol. 11, no. 2, pp. 439–448, Jun. 2017.
[57] C.-Y. Chow, M. F. Mokbel, and X. Liu, "Spatial cloaking for anonymous location-based services in mobile peer-to-peer environments," *GeoInformatica*, vol. 15, no. 2, pp. 351–380, 2011.
[58] A. Solanas, F. Sebé, and J. Domingo-Ferrer, "Micro-aggregation-based heuristics for p-sensitive k-anonymity: One step beyond," in *Proc. ACM Int. Workshop Privacy Anonymity Inf. Soc.*, 2008, pp. 61–69.

[59] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam, "*L*-diversity: Privacy beyond *k*-anonymity," *ACM Trans. Knowl. Discovery Data*, vol. 1, no. 1, p. 3, Mar. 2007.
[60] B. Bamba, L. Liu, P. Pesti, and T. Wang, "Supporting anonymous location queries in mobile environments with privacygrid," in *Proc. ACM Int. Conf. World Wide Web*, 2008, pp. 237–246.
[61] S. Mascetti, C. Bettini, X. S. Wang, D. Freni, and S. Jajodia, "ProvidentHider: An algorithm to preserve historical *k*-anonymity in LBS," in *Proc. IEEE Int. Conf. Mobile Data Manage., Syst., Services Middleware*, May 2009, pp. 172–181.
[62] B. Palanisamy and L. Liu, "Attack-resilient mix-zones over road networks: Architecture and algorithms," *IEEE Trans. Mobile Comput.*, vol. 14, no. 3, pp. 495–508, Mar. 2015.
[63] B. Ying, D. Makrakis, and H. T. Mouftah, "Dynamic mix-zone for location privacy in vehicular networks," *IEEE Commun. Lett.*, vol. 17, no. 8, pp. 1524–1527, Aug. 2013.
[64] R. Lu, X. Lin, T. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in VANETs," *IEEE Trans. Veh. Technol.*, vol. 61, no. 1, pp. 86–96, Jan. 2012.
[65] S. Gao, J. Ma, W. Shi, G. Zhan, and C. Sun, "TrPF: A trajectory privacy-preserving framework for participatory sensing," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 6, pp. 874–887, Jun. 2013.
[66] Z. Xu, H. Zhang, and X. Yu, "Multiple mix-zones deployment for continuous location privacy protection," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, Aug. 2016, pp. 760–766.
[67] J. Freudiger, M. H. Manshaei, J. Hubaux, and D. C. Parkes, "Non-cooperative location privacy," *IEEE Trans. Depend. Sec. Comput.*, vol. 10, no. 2, pp. 84–98, Mar./Apr. 2013.
[68] X. Gong, X. Chen, K. Xing, D.-H. Shin, M. Zhang, and J. Zhang, "From social group utility maximization to personalized location privacy in mobile networks," *IEEE/ACM Trans. Netw.*, vol. 25, no. 3, pp. 1703–1716, Jun. 2017.
[69] D. Yang, X. Fang, and G. Xue, "Truthful incentive mechanisms for *k*-anonymity location privacy," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 2994–3002.
[70] X. Gong, X. Chen, K. Xing, D.-H. Shin, M. Zhang, and J. Zhang, "Personalized location privacy in mobile networks: A social group utility approach," in *Proc. IEEE INFOCOM*, Apr./May 2015, pp. 1008–1016.
[71] K. Chatzikokolakis, C. Palamidessi, and A. Pazii, "Methods for location privacy: A comparative overview," *Found. Trends Privacy Secur.*, vol. 1, no. 4, pp. 199–257, 2016.
[72] G. Ghinita, "Privacy for location-based services," *Synth. Lectures Inf. Secur., Privacy, Trust*, vol. 4, no. 1, pp. 1–85, 2013.
[73] S. Zhang, Q. Liu, and G. Wang, "Enhancing location privacy through user-defined grid in location-based services," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, Aug. 2016, pp. 730–736.
[74] T.-H. You, W.-C. Peng, and W.-C. Lee, "Protecting moving trajectories with dummies," in *Proc. IEEE Int. Conf. Mobile Data Manage.*, 2007, pp. 278–282.
[75] P.-R. Lei, W.-C. Peng, I.-J. Su, and C.-P. Chang, "Dummy-based schemes for protecting movement trajectories," *J. Inf. Sci. Eng.*, vol. 28, no. 2, pp. 335–350, 2012.
[76] J. Krumm, "Realistic driving trips for location privacy," in *Proc. IEEE PerCom*, Mar. 2009, pp. 25–41.
[77] R. Chow and P. Golle, "Faking contextual data for fun, profit, and privacy," in *Proc. ACM Workshop Privacy Electron. Soc.*, 2009, pp. 105–108.
[78] H.-J. Do, Y.-S. Jeong, H.-J. Choi, and K. Kim, "Another dummy generation technique in location-based services," in *Proc. IEEE Int. Conf. Big Data Smart Comput. (BigComp)*, Jan. 2016, pp. 532–538.
[79] T. Hara, A. Suzuki, M. Iwata, Y. Arase, and X. Xie, "Dummy-based user location anonymization under real-world constraints," *IEEE Access*, vol. 4, pp. 673–687, 2016.
[80] S. Chen and H. Shen, "Semantic-aware dummy selection for location privacy preservation," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, Aug. 2016, pp. 752–759.
[81] C. A. Ardagna, M. Cremonini, E. Damiani, S. De Capitani di Vimercati, and P. Samarati, "Location privacy protection through obfuscation-based techniques," in *Proc. IFIP Annu. Conf. Data Appl. Secur. Privacy*, 2007, pp. 47–60.
[82] A. Gutscher, "Coordinate transformation—A solution for the privacy problem of location based services?" in *Proc. IEEE Int. Parallel Distrib. Process. Symp.*, Apr. 2006, pp. 7–13.
[83] R.-H. Hwang, Y.-L. Hsueh, and H.-W. Chung, "A novel time-obfuscated algorithm for trajectory privacy protection," *IEEE Trans. Serv. Comput.*, vol. 7, no. 2, pp. 126–139, Apr./Jun. 2014.
[84] M. Terrovitis and N. Mamoulis, "Privacy preservation in the publication of trajectories," in *Proc. IEEE Int. Conf. Mobile Data Manage.*, Apr. 2008, pp. 65–72.
[85] G. Ghinita, M. L. Damiani, C. Silvestri, and E. Bertino, "Preventing velocity-based linkage attacks in location-aware applications," in *Proc. ACM SIGSPATIAL Int. Conf. Adv. Geograph. Inf. Syst.*, 2009, pp. 246–255.
[86] M. Duckham and L. Kulik, "A formal model of obfuscation and negotiation for location privacy," in *Proc. IEEE PerCom*, May 2005, pp. 152–170.
[87] Y. Xiao and L. Xiong, "Protecting locations with differential privacy under temporal correlations," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2015, pp. 1298–1309.
[88] N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Optimal geo-indistinguishable mechanisms for location privacy," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2014, pp. 251–262.
[89] D. Kifer and A. Machanavajjhala, "No free lunch in data privacy," in *Proc. ACM SIGMOD Int. Conf. Manage. Data*, Jun. 2011, pp. 193–204.
[90] A.-M. Olteanu, K. Huguenin, R. Shokri, M. Humbert, and J.-P. Hubaux, "Quantifying interdependent privacy risks with location data," *IEEE Trans. Mobile Comput.*, vol. 16, no. 3, pp. 829–842, Mar. 2017.
[91] S. C. Soma, T. Hashem, M. A. Cheema, and S. Samrose, "Trip planning queries with location privacy in spatial databases," *World Wide Web*, vol. 20, no. 2, pp. 205–236, 2017.
[92] S. Amini, J. Lindqvist, J. Hong, J. Lin, E. Toch, and N. S. Cache, "Caché: Caching location-enhanced content to improve user privacy," in *Proc. IEEE Mobisys*, Jun./Jul. 2011, pp. 197–210.
[93] R. Shokri, G. Theodorakopoulos, P. Papadimitratos, E. Kazemi, and J.-P. Hubaux, "Hiding in the mobile crowd: Location privacy through collaboration," *IEEE Trans. Depend. Sec. Comput.*, vol. 11, no. 3, pp. 266–279, May/Jun. 2014.
[94] X. Zhu, H. Chi, B. Niu, W. Zhang, Z. Li, and H. Li, "MobiCache: When *k*-anonymity meets cache," in *Proc. IEEE Globecom*, Dec. 2013, pp. 820–825.
[95] B. Liu, W. Zhou, T. Zhu, L. Gao, T. H. Luan, and H. Zhou, "Silence is golden: Enhancing privacy of location-based services by content broadcasting and active caching in wireless vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 9942–9953, Dec. 2016.
[96] X. Zhang, X. Gui, and F. Tian, "A framework for measuring query privacy in location-based service," *KSII Trans. Internet Inf. Syst.*, vol. 9, no. 5, pp. 1717–1732, 2015.
[97] I. Wagner and D. Eckhoff. (2015). "Technical privacy metrics: A systematic survey." [Online]. Available: https://arxiv.org/abs/1512.00327
[98] M. Duckham and L. Kulik, "Simulation of obfuscation and negotiation for location privacy," in *Proc. Int. Conf. Spatial Inf. Theory*, 2005, pp. 31–48.
[99] Z. Ma, F. Kargl, and M. Weber, "Measuring long-term location privacy in vehicular communication systems," *Comput. Commun.*, vol. 33, no. 12, pp. 1414–1427, Jul. 2010.
[100] B. Hoh and M. Gruteser, "Protecting location privacy through path confusion," in *Proc. IEEE SecureComm*, Sep. 2005, pp. 194–205.
[101] C. Dwork, "Differential privacy: A survey of results," in *Proc. Int. Conf. Theory Appl. Models Comput.*, 2008, pp. 1–19.
[102] M. Li, R. Poovendran, K. Sampigethaya, and L. Huang, "Caravan: Providing location privacy for vanet," in *Proc. Embedded Security Cars (ESCAR) Workshop*, vol. 2. 2005, pp. 13–15.
[103] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, "Preserving privacy in GPS traces via uncertainty-aware path cloaking," in *Proc. ACM Conf. Comput. Commun. Secur.*, 2007, pp. 161–171.
[104] R. Shokri, G. Theodorakopoulos, C. Troncoso, J.-P. Hubaux, and J.-Y. Le Boudec, "Protecting location privacy: Optimal strategy against localization attacks," in *Proc. ACM Conf. Comput. Commun. Secur.*, 2012, pp. 617–627.
[105] *Mobile Location Apps Review*. Accessed: Nov. 30, 2016. [Online]. Available: http://www.webmapsolutions.com/mobile-location-apps/
[106] C. R. Vicente, D. Freni, C. Bettini, and C. S. Jensen, "Location-related privacy in geo-social networks," *IEEE Internet Comput.*, vol. 15, no. 3, pp. 20–27, May/Jun. 2011.
[107] *Foursqure*. Accessed: Dec. 21, 2016. [Online]. Available: https://foursquare.com/
[108] *Glympse*. Accessed: Dec. 21, 2016. [Online]. Available: https://www.glympse.com/
[109] *Twitter*. Accessed: Dec. 21, 2016. [Online]. Available: https://twitter.com/
[110] *Yelp*. Accessed: Dec. 21, 2016. [Online]. Available: https://www.tripadvisor.com.au/

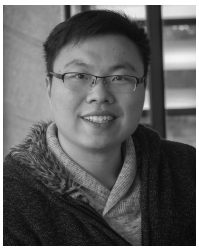
[111] M. Colbert, "A diary study of rendezvousing: Implications for position-aware computing and communications for the general public," in *Proc. ACM SIGGROUP Conf. Supporting Group Work*, 2001, pp. 15–23.
[112] E. Kaasinen, "User needs for location-aware mobile services," *Pers. Ubiquitous Comput.*, vol. 7, no. 1, pp. 70–79, 2003.
[113] G. Danezis, S. Lewis, and R. J. Anderson, "How much is location privacy worth?" in *Proc. WEIS*, vol. 5. 2005, pp. 1–13.
[114] H. Almuhimedi *et al.*, "Your location has been shared 5,398 times!: A field study on mobile app privacy nudging," in *Proc. ACM Conf. Human Factors Comput. Syst.*, 2015, pp. 787–796.
[115] K. Fawaz and K. G. Shin, "Location privacy protection for smartphone users," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2014, pp. 239–250.
[116] M. Mondal, Y. Liu, B. Viswanath, K. P. Gummadi, and A. Mislove, "Understanding and specifying social access control lists," in *Proc. Symp. Usable Privacy Secur.*, 2014, pp. 271–283.
[117] E. Snekkenes, "Concepts for personal location privacy policies," in *Proc. ACM Conf. Electron. Commerce*, 2001, pp. 48–57.
[118] P. Kumaraguru and L. F. Cranor, "Privacy indexes: A survey of Westin's studies," School Comput. Sci., Inst. Softw. Res. Int., Carnegie Mellon Univ., Pittsburgh, PA, USA, Tech. Rep. CMU-ISRI-5-138, Dec. 2005.
[119] K. Liu and E. Terzi, "A framework for computing the privacy scores of users in online social networks," *ACM Trans. Knowl. Discovery Data*, vol. 5, no. 1, p. 6, Dec. 2010.
[120] T. Minkus and N. Memon, "On a scale from 1 to 10, how private are you? scoring facebook privacy settings," in *Proc. Internet Soc. Workshop Usable Secur.*, 2014, pp. 1–6.
[121] J. Watson, H. R. Lipford, and A. Besmer, "Mapping user preference to privacy default settings," *ACM Trans. Comput.-Human Interact.*, vol. 22, no. 6, p. 32, 2015.
[122] J. Mugan, T. Sharma, and N. Sadeh, "Understandable learning of privacy preferences through default personas and suggestions," Inst. Softw. Res., Carnegie Mellon Univ., Pittsburgh, PA, USA, Tech. Rep. CMU-ISR-11-112, Aug. 2011.
[123] A. Sinha, Y. Li, and L. Bauer, "What you want is not what you get: Predicting sharing policies for text-based content on facebook," in *Proc. ACM Workshop Artif. Intell. Secur.*, 2013, pp. 13–24.
[124] M. Shehab and H. Touati, "Semi-supervised policy recommendation for online social networks," in *Proc. IEEE ASONAM*, Aug. 2012, pp. 360–367.
[125] I. Bilogrevic, K. Huguenin, B. Agir, M. Jadliwala, M. Gazaki, and J.-P. Hubaux, "A machine-learning based approach to privacy-aware information-sharing in mobile social networks," *Pervas. Mobile Comput.*, vol. 25, pp. 125–142, Jan. 2016.
[126] *Social Radar*. Accessed: Sep. 21, 2017. [Online]. Available: http://www.socialradar.com/
[127] *Yik Yak*. Accessed: Sep. 21, 2017. [Online]. Available: https://www.yikyak.com
[128] L. Ou, Z. Qin, Y. Liu, H. Yin, Y. Hu, and H. Chen, "Multi-user location correlation protection with differential privacy," in *Proc. IEEE 22nd Int. Conf. Parallel Distrib. Syst. (ICPADS)*, Dec. 2016, pp. 422–429.
[129] L. Fan and L. Xiong, "An adaptive approach to real-time aggregate monitoring with differential privacy," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 9, pp. 2094–2106, Sep. 2014.
[130] A. Mehmood, I. Natgunanathan, Y. Xiang, G. Hua, and S. Guo, "Protection of big data privacy," *IEEE Access*, vol. 4, pp. 1821–1834, 2016.
[131] S. Ren, K. He, R. Girshick, and J. Sun, "Faster R-CNN: Towards real-time object detection with region proposal networks," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 39, no. 6, pp. 1137–1149, Jun. 2017.



BO LIU (M'10) received the B.Sc. degree from the Department of Computer Science and Technology, Nanjing University of Posts and Telecommunications, Nanjing, China, in 2004, and the M.Eng. and Ph.D. degrees from the Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai, China, in 2007 and 2010, respectively. He was an Assistant Research Professor with the Department of Electronic Engineering, Shanghai Jiao Tong University, from 2010 to 2014, and a Post-Doctoral Research Fellow with Deakin University, Australia, from 2014 to 2017. He has been a Lecturer with the Department of Engineering, La Trobe University, since 2017. His research interests include wireless communications and networking, security and privacy issues in wireless networks.

WANLEI ZHOU (SM'09) received the B.Eng. and M.Eng. degrees from the Harbin Institute of Technology, Harbin, China, in 1982 and 1984, respectively, the Ph.D. degree from The Australian National University, Canberra, Australia, in 1991, all in computer science and engineering, and the D.Sc. degree from Deakin University in 2002. He is currently the Alfred Deakin Professor and the Chair of Information Technology, School of Information Technology. He has authored over 300 papers in refereed international journals and refereed international conferences proceedings. He has also chaired many international conferences.

TIANQING ZHU received the B.Eng. and M.Eng. degrees from Wuhan University, China, in 2000 and 2004, respectively, and the Ph.D. degree in computer science from Deakin University, Australia, in 2014. She was a Lecturer with Wuhan Polytechnic University, China, from 2004 to 2011. She is currently a Lecturer with the School of Information Technology, Deakin University, Australia. Her research interests include privacy preservation, data mining, and network security. She received the Best Student Paper Award in PAKDD 2014.



LONGXIANG GAO (M'13) received the Ph.D. degree from Deakin University, Australia. He was a Post-Doctoral Research Fellow with IBM Research, Australia. He is currently a Lecturer with the School of Information Technology, Deakin University. His research interests include mobile social networks, delay tolerant networks, and fog computing. His research works have been published in many international journals and conferences, such as the IEEE TRANSACTIONS ON MOBILE COMPUTING. He received the 2012 Chinese Government Award for Outstanding Students Abroad (Ranked No.1 in Victoria and Tasmania consular districts). He has served as the TPC co-chair, the publicity co-chair, the organization chair, and a TPC member for many international conferences.

YONG XIANG (SM'12) received the Ph.D. degree in electrical and electronic engineering from The University of Melbourne, Australia. He is a Professor and the Director with the Artificial Intelligence and Data Analytics Research Cluster, School of Information Technology, Deakin University, Australia. His research interests include information security and privacy, multimedia (speech, image, and video) processing, wireless sensor networks and IoT, and biomedical signal processing. He has authored two monographs, over 90 refereed journal articles, and numerous conference papers in these areas. He has served as the program chair, the TPC chair, the symposium chair, and the session chair for a number of international conferences. He is an Associate Editor of the IEEE SIGNAL PROCESSING LETTERS and the IEEE ACCESS.