Perils of Location Tracking? Personalized and Interpretable Privacy Preservation in Consumer Mobile Trajectories

Meghanath Macha
Information Systems and Management, Carnegie Mellon University, mmacha@cmu.edu

Beibei Li
Information Systems and Management, Carnegie Mellon University, beibeili@andrew.cmu.edu

Natasha Zhang Foutz
McIntire School of Commerce, University of Virginia, ynf8a@comm.virginia.edu

(Working Paper September 9, 2019)

Consumer location tracking is becoming omnipresent on mobile devices, producing vast volumes of behavior-rich location trajectory data. These data also grant data collectors, such as mobile app owners, a wide range of opportunities for monetization, such as location-based targeting by advertisers. However, this comes at a cost – potential invasion of consumer privacy. Existing approaches to privacy preservation are largely unsuited for these new data, not personalized, and difficult for data collectors to interpret the trade-off between privacy to consumers and utility to data users. We thus propose a personalized and interpretable framework to enable location data collectors to optimize the privacy-utility trade-off. Validating the framework on a sample of nearly one million location trajectories from more than forty thousand individuals, we find that high privacy risks indeed prevail in the absence of data obfuscation. For instance, a privacy attacker on average can accurately predict an individual's home address within a radius of 2.5 miles and mobile operating system with an 82% success. Moreover, 49% individuals' entire location trajectories can be fully identified by knowing merely two randomly sampled locations visited by that person. Outperforming multiple baselines, the proposed framework significantly reduces the privacy risk (e.g., by 15% of inferring home address) with minimal (i.e., $< 1\%$) decrease in an advertiser's utility. As novel and powerful consumer location trajectory data become increasingly leveraged, we demonstrate its value and accompanying privacy risk, and most importantly, propose an interpretable framework to mitigate its risk while maximizing its value.

Keywords: consumer privacy, GPS tracking, location data, mobile trajectory, machine learning, data obfuscation, mobile advertising

1. Introduction

1.1. Smart Tracking, Targeting, and Privacy

According to the latest Pew Research (Taylor and Silver 2019), 76% and 45% of the current population in the advanced and emerging economies, respectively, own a smartphone. These percentages continue to rise rapidly. Among the U.S. smartphone users, over 90% use location services like Google Maps (Pew 2016). The fast penetration of smartphones, combined with the wide adoption of location services, has produced a vast volume of behavior-rich mobile location data (location data, or trajectory data, hereafter). These data represent one of the latest, and most important, information sources available to marketers in the evolution of marketing data, from surveys to online clickstream and social media data (Wedel and Kannan 2016). It has also opened up $21 billion sales opportunities for advertisers, ranging from e-commerce retailers sending discount coupons to individuals in the vicinity of a store, commonly known as geo-fencing, to personal injury lawyers targeting those in emergency rooms (Luo et al. 2014, Andrews et al. 2016, Ghose et al. 2018, Kelsey 2018).

Location-based marketing is attractive to advertisers for multiple reasons. First, mobile location data are straightforward to collect – an app permission away and tracked in the background in most mobile ecosystems – and readily accessible to advertisers. While both Apple and Android have taken measures to limit the collection of location data, guidelines remain ambiguous about the sales of such data to advertisers (Apple 2014, Verge 2019). Second, mobile location data are superior to alternative location data. The build-in sensors of mobile devices can provide continuous tracking of the movement trajectory of an individual (i.e., a sequence of fine-grained location GPS coordinates). Such individual-level location trajectory data are more precise and granular than social media geo-tags and user self check-ins. It is also more representative of the population than the taxi and public transportation location data. Third, mobile location data offer an extensive profile of a consumer[1] for targeting purposes, such as his/her spatial-temporal movements thus rich contexts of his/her behaviors and brand preferences (Ghose et al. 2018), broad lifestyle patterns, socioeconomic conditions, and social relationships. Such offline data become even more powerful if combined with the consumer's online footprints, such as clickstream data or social media data, rendering a holistic online-offline consumer portfolio. Fourth, owing to excellent tracking and targeting of mobile advertising, attributing the success of a location-based ad campaign is simplified. Advertisers have access to a unique device ID associated with each smartphone, thus reducing advertisers' overhead to stitch together the users' data across sessions or apps when measuring the success of a campaign (Apple 2012).

[1] Throughout the paper, user and consumer are used interchangeably. They refer to an individual whose location is being tracked by a smartphone.

While we acknowledge the existence of diverse sources and varieties of mobile location data, the backbone of this rapidly growing mobile location data economy is the huge number of mobile applications (apps hereafter). App owners serve a two-sided market with consumers on one side and advertisers on the other, also collecting location data to offer better service to users and to monetize via location-based marketing with advertisers. For example, a recent article by the New York Times reported that data owners accrue half a cent to two cents per user per month from data acquirers (Valentino-Devries et al. 2018). While this powerful new form of human location and movement data benefit both data collectors and advertisers, they are also associated with consumer privacy risks (Wedel and Kannan 2016).

Merriam-Webster defines "privacy" as "the quality or state of being apart from company or observation." In business contexts, privacy broadly pertains to the protection of individually identifiable information online and offline, and the adoption and implementation of privacy policies and regulations. It is a key driver of online trust (Hoffman et al. 1999). In the context of online advertising, more than three-quarters of consumers surveyed believe that online advertisers have more information about them than they are comfortable with, and approximately half of them believe that websites ignore privacy laws (Dupre 2015). For location data, privacy risks are exemplified by identifications of an individual's home address, daily movement trajectories, and broad lifestyle, as vividly depicted by a recent New York Times' article (Valentino-Devries et al. 2018). These risks are debatably more concerning than those associated with the more conventional forms of consumer data, such as an individual's media entertainment viewing, single credit card's history, social media contents, or online clickstreams.

Consumers have historically leveraged a variety of tools, such as caller ID, spam filters, pop-up blockers, anonymous browsing, or location tracking blockers, to protect their privacy. Despite widespread privacy concerns, privacy laws and security technologies have not kept pace with data collection, storage, and processing technologies. This has resulted in an environment in which high profile security breaches and misuse of private consumer information are prevalent. In the past decade, more than 5,000 major data breaches have been reported, with the recent examples of Facebook, Sony, Ashley Madison, and Marriott. Each data breach is also costly, estimated to be around $4 million (Wedel and Kannan 2016). Protecting privacy is thus increasingly becoming a key concern for firms and regulatory bodies. Besides strengthening privacy regulations, more research is called for to develop privacy-friendly data storage, processing, and analysis technologies (Wedel and Kannan 2016).

While loss of privacy in certain contexts entails predominantly negative costs for consumers, in many others results in both negative costs and positive benefits to consumers. For instance, a looser privacy setting allows a user to reach a wider audience on social media for information acquisition or

propagation (Adjerid et al. 2018), receive better services and increased personalization (Chellappa and Shivendu 2010), or financial benefits such as coupons (Luo et al. 2014, Ghose et al. 2018) or lower insurance premiums (Soleymanian et al. 2019). Hence, a data collector needs to trade off between consumer privacy and data accessibility, accuracy, and usability (Muralidhar and Sarathy 2006). The unique properties of, and hence challenges brought by, mobile location data, that we will detail later, also call for a new framework to accomplish this tradeoff. We thus aim to develop such a framework that balances consumer privacy and data usability to advertisers while tackling the unique challenges inherent in the increasingly accessible and important mobile location data.

The conflict of interest between consumer privacy and location-based targeting constitutes part of a larger debate over tracking and targeting on digital platforms that have resulted in actions from both industries and regulatory bodies. In 2016, Apple, with 44.6% US smartphone market share (Statista 2018), introduced limited ad tracking (LAT), which allows users to opt out of tracking indefinitely (Apple 2016). Following suit, Android, the second most adopted mobile ecosystem rendered more controls to each user to limit tracking in the latest software update (Verge 2019). European Union's General Data Protection Regulation (GDPR, Regulation (2016)), effective from May 2018, requires users to opt-in (rather than opt out of) behavioral targeting and gives explicit permission for their data to be shared across firms. Against this background, our study provides empirical evidence and practical solutions to inform the ongoing debate over mobile location tracking and location-based targeting.

1.2. Research Agenda and Challenges

Consistent with the extant literature across multiple disciplines on data sharing (Li et al. 2012, Terrovitis et al. 2008, Li and Sarkar 2009, Chen et al. 2013, Yarovoy et al. 2009, Machanavajjhala et al. 2009), we assume that a data collector is primarily responsible for preserving consumer privacy before sharing the data with advertisers[2]. In an ideal scenario, all entities involved – smartphone manufacturers and operating system providers, location data collectors, and advertisers – should invest in ensuring privacy. Nonetheless, while smartphone manufactures and operation system providers may limit location data collections, many mobile apps, particularly those focused on location-based services, would require users to opt-in to data tracking for enhanced experiences. For instance, an app that helps a user find nearby gas stations or restaurants would be less useful if the suggestions were not based on the user's present location. Therefore, location data collectors,

[2] The proposed framework is applicable to other contexts as well, such as when the data collector conducts location-based marketing for itself or advertisers without sharing the data with advertisers, or when a third-party data aggregator acquires location data across multiple data collectors in order to monetize the data. Nonetheless, we acknowledge that this framework is one of many potential solutions to the privacy-utility trade-off facing a location data collector.

such as mobile app owners, essentially offer a grassroots solution since they are the ones who collect the location data and monetize it. We thus take a data collector's perspective, identify the key issues facing it, and propose an end-to-end framework that balances between protecting consumer privacy against any entity with malicious intents and preserving advertisers' targeting capabilities. In summary, we answer the following questions.

1. *Consumers' privacy risks:* What are the different privacy risks of location tracking to consumers? Can these risks be quantified for each consumer? Since a data collector has limited purview of how an advertiser could link the location data to a consumer's private information, understanding and quantifying the risks associated with various types of privacy breaches (or attacks, threats, hereafter) is essential to perform necessary data obfuscations.

2. *Advertisers' utilities:* What types of behavioral information can be extracted from consumers' location data? What is the value of this information to an advertiser's targeting ability?

3. *Data collector's trade-off between consumers' privacy risks and advertisers' utilities:* Is there a reasonable privacy-utility trade-off? If yes, what are the necessary steps that a data collector needs to take to ensure this?

From a methodological standpoint, the questions we study broadly fall under the paradigm of Privacy-Preserving Data Publishing (PPDP) – data sharing[3] by ensuring both consumer privacy and data utility. PPDP has been widely studied in the context of relational databases (cf. (Fung et al. 2010) for an extensive survey). However, the uniqueness of location data, such as high dimensionality (due to a large number of locations visited), sparsity (fewer overlap of locations across users) and sequentiality (order of locations visited), poses additional challenges (Chen et al. 2013). Traditional k-anonymity, which ensures that a user record is indistinguishable from at least $k-1$ records and its extensions face the curse of high dimensionality while dealing with granular, sometimes second-by-second, location data (Aggarwal 2005). $\epsilon-$differential privacy anonymization[4] and other obfuscation techniques, often achieved by randomization mechanisms (Machanavajjhala et al. 2006), fail to preserve the truthfulness of the location data, rendering the obfuscated data less useful for an advertiser's visual data mining tasks. More recent local obfuscation techniques (Chen et al. 2013, Terrovitis et al. 2017)[5] provide a good privacy-utility balance. However, the obfuscation mechanisms are often complex for a data collector to interpret and apply in practice. For instance, the $(K, C)_L$ privacy framework (Chen et al. 2013) requires multiple parameters from a

[3] Throughout the paper, sharing and publishing are used interchangeably.

[4] $\epsilon-$differential privacy ensures that addition or deletion of a single consumer record does not have a significant effect on the outcome of analysis and thus ensures a customer record is indistinguishable from other records.

[5] The main idea in such techniques is to assign a score that captures both privacy risk and utility for each location visited by a user and suppress the locations with lower scores, that is, lower trade-off.

data collector – probability thresholds of a privacy attacker to succeed in different types of attacks. LSup proposed by (Terrovitis et al. 2017) requires similar input parameters. Given the complex nature of these approaches, understanding and setting such parameters are non-trivial for a data collector. Hence, a more interpretable framework is needed to assist a data collector.

Furthermore, an advertiser's utility in the extant approaches is not tied to specific business use cases. These approaches, devised mostly from the Computer Science literature, measure an advertiser's utility by the number of unique locations or location sequences preserved in the obfuscated data (Chen et al. 2013, Terrovitis et al. 2017). These measures are rather rudimentary and impractical for advertisers to interpret or link to monetary decision-making. This challenge needs to be tackled by tying the advertiser's utility to real-world business contexts. We will next overview our framework that addresses the above challenges.

1.3. Overview of Proposed Framework

We provide a brief overview of the proposed framework that consists of three main components: privacy risk quantification, data utility computation, and obfuscation scheme.

Privacy Risk Quantification. In risk quantification, we quantify the privacy risk associated with each user based on the visited locations and the corresponding timestamps. Specifically, we compute the risk for two classes of privacy attacks: "sensitive attribute attack", where a privacy attacker aims to infer a user's sensitive attributes such as the home address (Li et al. 2007, Tucker 2013, Gardete and Bart 2018, Rafieian and Yoganarasimhan 2018), and "re-identification attack", where an attacker tries to identify all the locations visited by a user based on a subset of the visited locations (Samarati 2001, Pellungrini et al. 2018).

Data Utility Measurement. To assess the utility of the location data, we follow the marketing literature to consider a popular business goal – POI recommendations in mobile advertising. Reliable predictions of a consumer's future locations would enable an advertiser to target the consumer with relevant contextual contents (Ghose et al. 2018). For instance, if a chain restaurant can accurately predict that a consumer is going to be in the vicinity of one of the outlets, it may target the consumer with a discount coupon. In this research, we measure the utility as the accuracy of the neighborhood-based, collaborative filtering recommendation model learned on the location data. The key idea of this recommender is to identify other consumers with similar historical preferences (i.e., neighbors) to infer the focal consumer's future preferences (Bobadilla et al. 2011)

Obfuscation Scheme. We leverage each user's risk computed in the earlier risk quantification step and introduce a decision parameter to devise a user-specific suppression score. The score is used to suppress (i.e., obfuscate) a subset of locations visited by a user. The suppression, while ensuring a reduction in the overall risk associated, also adversely affects the utility. Thus, we empirically determine the parameter which provides a privacy-utility trade-off.

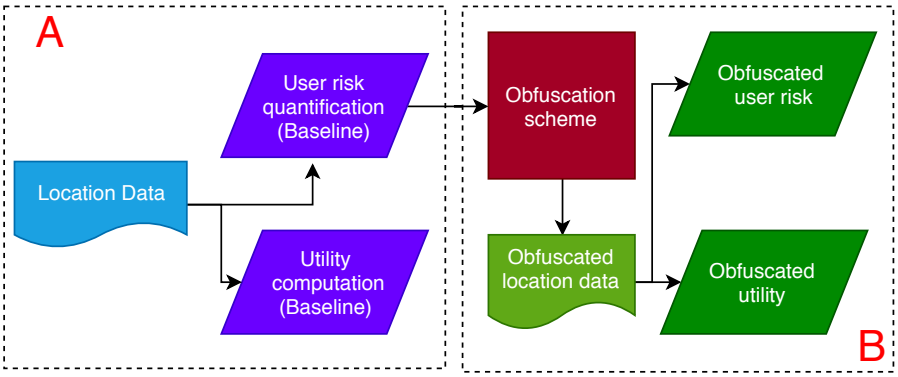


Figure 1 Overview of the proposed framework

In summary, Figure 1 illustrates the proposed framework with the three components discussed above. In Part A, we compute the user risk and advertiser utility associated with the non-obfuscated location data (i.e., the full sample). These would represent the counterfactual case when no privacy protection is performed. We expect the full sample to demonstrate the maximum utility that an advertiser could potentially gain from the location data and maximum consumer risk if the data were published as is. In Part B, we devise the user-level suppression scores using the risk scores computed on the full sample and perform obfuscation at an individual user level. We repeat the computation of risk and utility by varying the heuristic decision parameter to empirically determine the best trade-off between user privacy and data utility.

Note that while we illustrate the proposed framework by considering the most commonly encountered two classes of privacy threats and one advertiser use case, the framework is flexible to accommodate other types of privacy attacks and use cases. For example, the risk quantification can be performed for variations of the "re-identification" attack. To exemplify, consider a privacy attack to infer a user's location sequence or visit frequency to a specific location. The user's privacy risk can be quantified either analytically or by leveraging the existing machine learning heuristics for these attacks (Pellungrini et al. 2018). Also, the advertiser utility may be computed as the predictive accuracy for other different business applications (e.g., when is a consumer most likely to convert based on her past location trajectory), or the advertiser's incremental revenues gained from the location-based mobile targeting.

We will briefly summarize our empirical findings next.

1.4. Summary of Key Findings

We validate the proposed framework on a unique data set of nearly one million mobile locations from over 40,000 individuals in a major mid-Atlantic metropolitan area in the U.S. over a period of five weeks in 2018. The main findings are summarized as follows.

First, regarding the privacy risk, we find that the absence of an obfuscation scheme, that is, no steps taken by a data collector to ensure consumer privacy, indeed entails high risks of privacy

invasion. On average, the probability of a successful privacy attack is 83% in inferring consumer sensitive information and 49% in re-identifying consumer entire location trajectory, respectively. More specifically, a privacy attacker on an average could accurately predict a customer's sensitive information including home address in a radius of 2.5 miles and mobile operating system[6] with an 82% success. Moreover, we find high re-identification privacy risk. For example, 49% individuals' entire location trajectories can be fully identified by knowing only two randomly sampled locations visited by each person[7].

Second, regarding the data utility, we find significant value of the data to advertisers. An advertiser aiming to target consumers by identifying the next location most likely visited by a consumer would be able to predict it with 25% success. This means that by analyzing the behavioral patterns revealed by the historical location trajectories, for every one out of four customers, businesses are able to design a highly precise geo-targeting strategy.

Finally, a data collector could curtail this invasion of consumer privacy by performing obfuscations. Using the proposed obfuscation scheme, a data collector has multiple trade-off options to choose from to perform the obfuscation. We find that the proposed framework presents a better choice set compared to several baseline approaches using rule-based heuristics. For instance, when a privacy attacker aims to predict a user's home address, the proposed obfuscation scheme reduces the risk to user privacy by 15% (maximum decrease when compared to several baselines) with less than 1% decrease in the advertiser's utility (minimum decrease). We present a more detailed discussion of the empirical findings and comparison with other baseline obfuscation schemes in Section 5.

1.5. Summary of Contributions

We propose an interpretable framework built on the principles of personalized data obfuscation for the emerging and increasingly important mobile location data. Conceptually, this research demonstrates the importance for location data collectors to preserve both consumer privacy and advertiser utility on a two-sided market; and a systematic framework to accomplish the privacy-utility balance. It also stands among the first research to demonstrate the immense business value of the novel mobile location trajectory data that capture human daily movement and will be increasingly leveraged by marketers and other entities, such as municipalities for smart city planning. It simultaneously illustrates the significant privacy risks associated with these data if no framework is in

[6] Previous surveys have shown a strong relationship between mobile operating system and consumer demographics.(eMarketer 2013)

[7] Note that these numbers are all estimated based on machine learning heuristics, which requires merely the consumers' locations and corresponding timestamps as the inputs. Hence, any entity, including advertisers, that has access to the data could accomplish the same.

place to preserve consumer privacy. Managerially, this framework tackles three inter-related, critical challenges facing location data collectors: consumer risk quantification, data utility measurement, and data obfuscation. It offers data collectors multiple, interpretable, and personalized options that require only parsimonious input to protect consumer privacy while preserving advertiser utility, hence overall monetization opportunities for data collectors.

Methodologically, this framework (1) quantifies privacy risks by extracting a comprehensive set of features from the location trajectory data, thus accommodating varieties of privacy attacks and allowing identifications of which features contribute the most to privacy risks; (2) measures data utilities by tying to real-world business use cases, such as POI recommendations shown to improve retailers' incremental revenues (Ghose et al. (2018)); (3) proposes an obfuscation scheme that suppresses locations at an individual level based on each person's distinct privacy risk and introduces a heuristic decision factor to data collectors with multiple options of privacy-utility trade-off, thus intuitive and interpretable to data collectors; (4) demonstrates efficacy via validation on a real-world location trajectory data set collected from large number of individuals over an extended period and comparison with benchmarks.

The rest of the paper is organized as follows. In Section 2, we review literature in various disciplines relevant to the problem studied in our work. In Section 3, we provide details of our business setting and discuss sampling and summary statistics of the location data we analyze. In Section 4, we introduce our framework for privacy preserving data sharing with three main components (Figure 1). In Section 5, we discuss our empirical results and compare with several baselines, and detail the advantages of our proposed methodology. We provide concluding remarks in Section 6.

2. Literature Review

We will concisely review the most relevant Marketing, Management, Information Systems (IS), and Computer Science (CS) literature on privacy, privacy-preserving methodology, and mobile location-based advertising.

2.1. Literature on Consumer Privacy

The marketing literature has a historical, and newly revived, interest in consumer privacy. As different forms of marketing data emerge over time, this literature has examined privacy concerns that arise in many marketing contexts and data forms, such as marketing research like surveys (Mayer and White Jr 1969, De Jong et al. 2010, Acquisti et al. 2012), direct marketing via phones or emails (Hann et al. 2008, Kumar et al. 2014, Goh et al. 2015), offline retail sales (Schneider et al. 2018), subscription services and various customer relationship management (CRM) programs (Conitzer et al. 2012), online personalization services in computers and mobile devices (Chellappa

and Shivendu 2010), online search and transactions (i.e. e-commerce) (Bart et al. 2005), online social networks (Adjerid et al. 2018). Prior studies have also examined privacy topics related financial and healthcare marketing, such as crowd-funding (Burtch et al. 2015), credit transactions, insurance (Garfinkel et al. 2002, Soleymanian et al. 2019), and health care (Garfinkel et al. 2002, Miller and Tucker 2009, 2017). As marketers commonly leverage customer private information for behavior-based advertising and target, the latest research has also investigated online, social media, and mobile advertising (Goldfarb and Tucker 2011a,b,c, Conitzer et al. 2012, Tucker 2013, Gardete and Bart 2018, Rafieian and Yoganarasimhan 2018). Broadly speaking, any circumstances that involve customer databases would entail privacy concerns and needs for privacy protection (Garfinkel et al. 2002, Martin et al. 2017, Muralidhar and Sarathy 2006, Qian and Xie 2015). Beyond business-to-consumer (B2C) contexts, even business-to-business (B2B) platforms incur privacy concerns and requires effective strategies to address such concerns (Kalvenes and Basu 2006). Marketing research on privacy has fallen into four streams: consumer-, firm-, regulation-, and methodology- focused. We will concisely review each.

The first stream takes consumers' perspectives, and as a result, derives implications for firms on designing optimal privacy-friendly policies. For instance, this literature has studied how consumers respond to privacy concerns or make privacy choices about, such as privacy-intruding survey questions (Acquisti et al. 2012), platform provided privacy settings (Burtch et al. 2015, Adjerid et al. 2018), or online display ads that match the website contents but with obtrusive format (Goldfarb and Tucker 2011c,b), opt-in/out options of email marketing program (Kumar et al. 2014). It also studies how normative and heuristic decision processes influence consumers privacy decision making (Adjerid et al. 2016). Overall, this research points to the positive effect of granting consumers enhanced controls over their own privacy, such as increasing their likelihood of responding to sensitive survey questions or click on personalized ads (Tucker 2013).

The second stream of literature take firms' perspectives, often using a game-theoretic approach to reach normative implications of firms privacy policies. For instance, Chellappa and Shivendu (2010) derive the optimal design of personalization services for customers with heterogeneous privacy concerns. Gardete and Bart (2018) propose the optimal choice of ad content and communications when firm withholds customers private information. Conitzer et al. (2012) reveal a monopolys optimal cost of privacy for customers to remain anonymous. Hann et al. (2008) show that consumers' different actions toward preserving their privacy, such as address concealment or deflecting marketing, impact a firms actions to either shifting marketing toward other consumers or reduce marketing overall. Adding competition to the picture, this stream of research also suggests optimal competitive strategies when profiting from disclosing customer information (Casadesus-Masanell and Hervas-Drane 2015), or designing a B2B market which preserves privacy to incentivize competitor

participation (Kalvenes and Basu 2006). Other studies have also conceptualized the differential importance of privacy to different platforms (Bart et al. 2005) and assessed the impact of data breaches on firms financial performances (Martin et al. 2017). Interestingly, this stream of research also demonstrates that firms, such as an ad network, do have innate incentives to preserve customer privacy even without privacy regulations (Rafieian and Yoganarasimhan 2018).

The third stream of research focuses on privacy regulations. For example, privacy regulations impact firms privacy-pertinent practices, technology innovations (Adjerid et al. 2016) and adoptions (Miller and Tucker 2009, 2017), and consumer responses such as to do-no-call registry (Goh et al. 2015). (Goldfarb and Tucker 2011a) show that the European Union (EU)s privacy policy reduces the online display ads effectiveness. On the other hand, different components of a privacy law may incur different effects, for instance, granting users control over re-disclosure encourages the spread of adoption of genetic testing, whereas privacy notification deters individuals from obtaining genetic tests (Miller and Tucker 2017).

The fourth stream of research examines a wide range of methodologies that regulatory bodies and firms may engage to address privacy concerns. These methods fall under two broad categories: without data obfuscation and with as our research. Without data obfuscation, these methods largely involve firms altering consumers privacy perceptions, hence alleviating privacy concerns. Examples include altering the order of survey questions (Acquisti et al. 2012), revealing other consumers attitudes towards privacy (Acquisti et al. 2012), altering the labels of privacy-protecting options (Adjerid et al. 2018), offering opt-in/out options (Kumar et al. 2014), granting enhanced privacy controls over, for instance, personally identification information (Tucker 2013), allowing customers to remain anonymous with a cost (Conitzer et al. 2012) or granting aggregate instead of granular information (Sandıkçı et al. 2013). Consumers themselves may also take actions, such as declining to answer certain survey questions, concealing their addresses, or deflecting marketing solicitation to preserve privacy (Hann et al. 2008). Governments all around the world are also providing regulatory protections, such as do-no-call registry (Goh et al. 2015) and instating state genetic privacy laws (Miller and Tucker 2017).

Other methodologies, on the other hand, leverage data obfuscation to the original data or query outputs. Our work closely relates to this stream of work. Hence, we provide a more thorough survey of these works by breaking down the literature into relational data and location data methodologies.

2.2. Relational Data Obfuscation

Relational databases have a fixed schema. For instance, medical records of a patient or census data, where the number of attributes/columns are fixed could be stored in a relational database. These are different from a location database where different users could have a varied number of locations

visited (hence varying schema). Privacy-preserving data sharing methods in relational databases has been studied extensively in the IS and CS literature.

Heuristic-based approaches aim to preserve consumer privacy against definitive notions of privacy attacks in relational databases. k-anonymity(Samarati and Sweeney 1998) protects users from re-identification threats by obfuscating published data such that a user record is indistinguishable from at least k-1 records. ℓ-diversity (Machanavajjhala et al. 2006) and confidence bounding (Wang et al. 2007) aim to prevent privacy attackers from sensitive attribute inference threats. ℓ-diversity ensures this by obfuscating data so that sensitive attributes are well represented for each user identifier, while confidence bounding limits an attacker's confidence of inferring a sensitive value to a certain threshold. Li and Li (2008) mimic a privacy attacker by mining negative association rules from data to use them in the anonymization process. These traditional heuristics suffer from the curse of high dimensionality (*Aggarwal* 2005) in the context of trajectories reducing an advertiser's utility. To address this issue, variations of k-anonymity such as k^m-anonymity (Terrovitis et al. 2008) and complete k-anonymity (Bayardo and Agrawal 2005) have been proposed for high dimensional transaction data. However, these techniques only address identification attacks and are still vulnerable to sensitive attribute attacks. Slicing techniques aimed at transactional databases (Li et al. 2012, Wang et al. 2018) work by vertically and horizontally partitioning a database into several slices that meet the privacy-preserving requirement. A modified random response model was developed to allow respondents the opportunity to conceal their truthful answers in order to measure socially sensitive consumer behavior and correct for social desirability bias (De Jong et al. 2010). While these techniques work well for high dimensional data, they do not explore obfuscation of temporal information which is crucial in extracting behavioral information from location data.

Another line of work aims to achieve the uninformative principle - shared data should provide an attacker with as little additional information as possible beyond their background knowledge. The primary difference to heuristic-based approaches is that these works have a stricter notion of privacy and aim to protect user privacy from arbitrary background knowledge. Differential privacy (Dwork and Lei 2009) paradigm is well-known in this context. Information-theoretic approaches quantitatively measure privacy risk based on various entropy-based metrics, such as conditional entropy (Sankar et al. 2013, Li and Sarkar 2009) and mutual information (Yang et al. 2018, Menon and Sarkar 2007, Li and Sarkar 2013, 2006) and design obfuscation techniques aimed at minimizing these measures in published data. Perturbation methods (Muralidhar and Sarathy 2006)[8], data shuffling[9], or a combination of perturbation and data shuffling (Qian and Xie 2015) have also

[8] Perturbation techniques add a small noise to the original data to ensure that the privacy risk is minimized.

[9] Shuffling is usually performed across user rows or columns. For instance, a subset of a user record is replaced with another user's record to minimize privacy risk.

been proposed. For instance, Garfinkel et al. (2002) perturb the database query answer to have the correct answer probabilistically or deterministically embedded in the range of the perturbed answers. Muralidhar and Sarathy (2006) employ data shuffling for condential numerical data where the values of the condential variables are shufed among observations, while preserving a high level of data utility and minimizes the risk of disclosure. Schneider et al. (2018) develop a Bayesian probability model to produce synthetic data. Public key encryption, digital certificate, and blinded signatures are also common privacy-friendly tools (Kalvenes and Basu 2006). A critique against the perturbation techniques is that they do not preserve the truthfulness of location data, hindering marketer's ability to perform visual data mining tasks (Fung et al. 2010). Li and Sarkar (2009) propose a tree-based pruning technique to protect consumers against sensitive attribute attacks but do not consider the risk associated with re-identification attack. Menon and Sarkar (2007) and Li and Sarkar (2013, 2006) primarily aim at anonymizing categorical data and would face sparseness and computational issues in the context of location data. Muralidhar and Sarathy (2006) propose a data shuffling technique to overcome the concerns regarding perturbation techniques but this approach is limited to numerical data. In our problem setting, we assume that a data collector has enough knowledge about the privacy attacker and thus advocate definitive notions of privacy threats.

2.3. Location Data Obfuscation

Researchers, primarily from CS, have proposed extensions of the traditional heuristics to preserve privacy in location data generated from simulated/synthetic data (Chen et al. 2013, Terrovitis et al. 2008, Abul et al. 2008, Yarovoy et al. 2009), truck/car movements (Abul et al. 2008, Yarovoy et al. 2009), or social media check-in data (Terrovitis et al. 2017, Yang et al. 2018). The seminal work by (Abul et al. 2008) proposes (k, δ) anonymity where the idea is to perform space generalization on location data. The user trajectories are transformed so that k of the trajectories lie in a cylinder of the radius δ. (Yarovoy et al. 2009) present a variation of k-anonymity for moving object databases (MOD) based on the assumption that MODs do not have a fixed set of quasi-identifiers (QIDs). They define the timestamps of locations as QIDs and propose two obfuscation techniques based on space generalization. Both these works aim at protecting users from re-identification attacks. In our problem, we consider both sensitive attribute attack as well as re-identification attack.

More recently, suppression techniques have garnered attention in anonymizing location trajectory data (Chen et al. 2013, Terrovitis et al. 2008, 2017). In the seminal work, Terrovitis et al. (2008) develop a local suppression anonymization technique assuming an attacker holds partial user trajectories similar to the setting of re-identification attack in our study. Building on Terrovitis et al. (2008), the authors propose both global, local suppression and splitting obfuscation techniques

in Terrovitis et al. (2017). Chen et al. (2013) propose $(K, C)_L$ privacy framework that provides privacy guarantees against both identity and attribute linkage attacks. The model requires three parameters from a data collector - probability thresholds of a privacy attacker succeeding in the two types of attacks along with a parameter corresponding to an attacker's background knowledge. The utility of the data in Chen et al. (2013) and Terrovitis et al. (2008, 2017) is measured by the number of unique location points or frequent sequences preserved in the published data.

Our study distinguishes itself from this prior methodological research in three major aspects: First, compared to prior work our method requires only intuitive and parsimonious input regarding the cardinality of partial trajectories (see Section 4.1.3 for a more detailed explanation) for computation of risk and obfuscation of trajectory data. Second, instead of using the number of unique location points or frequent sequences as rudimentary measurements, we measure the location data utility in a real-world business setting by using the predictive performance in POI recommendation, which has been shown to be an effective strategy to improve retailers incremental revenues by prior mobile advertising literature (e.g., Ghose et al. (2018)). Third, our data obfuscation scheme is intuitive and interpretable to business managers. We introduce a heuristic decision factor to provide a data collector with multiple trade-off options between user privacy risk and data utility.

2.4. Location-based Mobile Advertising

Finally, our work is related to mobile marketing and location-based advertising research. Using randomized field experiments, researchers have demonstrated that mobile advertisements based on location and time information can significantly increase consumers likelihood of redeeming geo-targeted mobile coupons (Fang et al. 2015, Molitor et al. 2019, Fong et al. 2015b, Luo et al. 2014). In our framework, we measure utility of location data to an advertiser by considering a popular business application - POI Recommendation. Identifying the next location a consumer is likely to visit based on consumer location trajectories is crucial to perform such behavioral targeting. In a recent paper by Ghose et al. (2018), the authors designed a POI-based mobile recommendation based on similarity in consumer mobile trajectories and demonstrated that such a strategy can lead to a significant improvement in retailer's incremental revenue. Recent studies have also shown that understanding consumers' hyper-context, for example the crowdedness of their immediate environment (Andrews et al. 2016), weather (Li et al. 2017) or the competitive environment (Fong et al. 2015a, Dubé et al. 2017), is critical to marketers' evaluation of mobile marketing effectiveness. Previous studies have also examined consumer perceptions and attitudes toward mobile location-based advertising (Bruner and Kumar 2007, Xu 2006).

3. Background and Data

We partner with a leading location data collector in the U.S. that aggregates location data across hundreds of mobile apps covering one-fifth of the U.S. population across Android and iOS operating systems.

3.1. Business Setting

There are three key entities in our business setting.

1. User: is an individual who owns a smartphone with one or more of the apps installed that transmit the individual's location data to the data collector. Each user has the option to opt out from any app's location tracking, with some potential downsides of reduced utilities from using certain app functions, such as maps or local restaurant finders.

2. Data collector: is an entity that tracks and collects users' location data from mobile apps. They can be mobile app owners or a data aggregator that integrate location data from multiple apps. The data are collected in real time and then may be shared/sold to advertisers interested in targeting the users. In our setting, the data collector is primarily responsible for ensuring a trade-off between consumer privacy and advertisers' utility.

3. Advertisers: are firms that acquire data from a data collector to improve the targetability of their marketing campaigns. In our context, we assume that a third party, or even a subset of these advertisers, might be adversarial (henceforth "privacy attackers") – who have an intent to perform malicious activities on the shared location data to invade consumer's privacy. Such intent may be due to, for example, over-aggressive marketing objective or ignorance of privacy concern.

3.2. Data

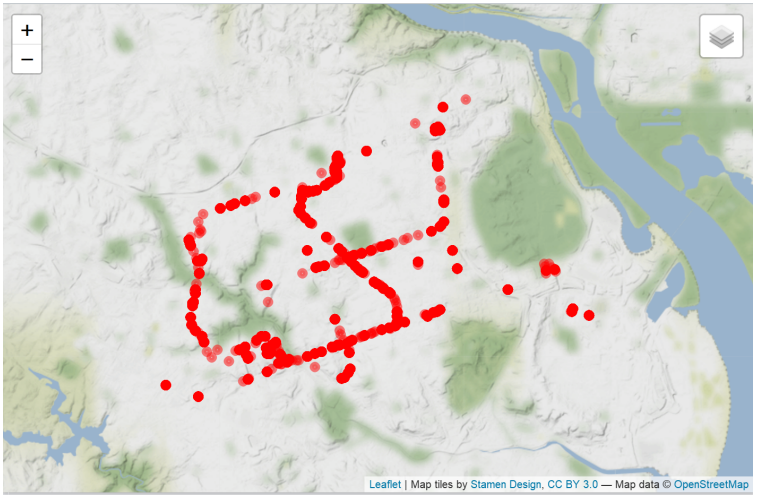


Figure 2 **An example of a user's footprints with 732 unique locations over the five-week observation period.**

Description	Mean (sd)	Min (Max)
Number of locations per user	23.47 (50.26)	2 (1104)
Number of unique locations per user	22.96 (49.09)	2 (963)
Overall duration (in hours)	272.97 (278.25)	0.05 (759.27)
Duration at each location (minutes)	27.96 (45.99)	1.6 (359.23)
Distance between locations (in km)	1.89 (3.89)	0.2 (75.49)

Table 1 Summary statistics of our location data

The location data we analyze cover a major mid-Atlantic metropolitan region in the U.S. Figure 2 shows an example of the geographical map of a user from our data with 732 unique locations visited in the observation period. In total, we have 940,000 observations from 40,012 users observed over a period of five weeks in September-October, 2018. Each row of the data corresponds to a location recorded for a user. Each row contains information about

- User ID: a unique identifier of an individual using a mobile app.
- Platform ID: Identifier of the mobile operating system, Android or iOS.
- Latitude and longitude of the location.
- Timestamp of the location.
- Opted out: Indicator whether a user has opted out from tracking.
- Time spent: The service pings mobiles in frequent intervals to determine the amount of time spent at each location.

3.2.1. Sample Selection and Summary Statistics We randomly sample 50% of all users in the data (20,000 users) and all their location data for training and cross-validating our machine learning models (Details discussed in Section 5.1 and Appendix A). Based on the models and parameters learned, we then conduct the main analysis using the rest 50% of the data (remaining 20,012 users and their location data). Table 1 has summary statistics of the data. On average, a user has 23.47 locations and 22.96 unique locations. To reduce phone battery drainage, data redundancy and storage cost, the data collector pings each user's smartphone frequently but only logs a location when there is a significant change in the user's GPS coordinates. This also helps estimate the amount of time spent by a user at each logged location. The average total time spent by a user at various locations is 273 hours[10] (1.6 weeks). We compute the distance between two

[10] The overall observation period of our sample is five weeks. However, some users may have been tracked for a shorter period of time. For instance, a user who installs an app in the third week of our observation period would be tracked for the next two weeks.

consecutive locations by converting the latitude and longitude to the Universal Transverse Mercator (UTM) coordinates and then take the Euclidean distance. On average, the distance between the consecutively tracked locations is 1.89 km.

3.2.2. Uniqueness of Mobile Location Data The existing literature on privacy-preserving sharing of location data, primarily from the CS discipline, have tested the methodologies on either simulated data (Chen et al. 2013, Terrovitis et al. 2008, Abul et al. 2008, Yarovoy et al. 2009), or truck/car movements (Abul et al. 2008, Yarovoy et al. 2009), or social media check-in data (Terrovitis et al. 2017, Yang et al. 2018), also merely over a short period such as 24 hours. We make an initial effort to develop a privacy-preserving framework for, and validate it on, a real-world human physical movement data. Such data, as aforementioned, are automatically tracked on mobile devices, often via wifi and GPS etc. multi-technology triangulation, and thus more precise than social media geo-tags and consumer manual location check-ins; they are also more representative of the general population than what the taxi or public transportation data reflect, hence much more valuable to advertisers and other data users. On the other hand, their massive scale, in our case nearly one million mobile locations from over 40,000 individuals over five weeks, also entails unique challenges, as discussed earlier, hence imminent needs to develop a new framework to address these challenges.

3.3. Privacy Attacks

The notion of privacy threats in the prior literature can be broadly broken down into two categories (Fung et al. 2010). The first category has definitive notions of privacy. For instance, a user's privacy is at risk when an attacker is able to link a user to a record (re-identification attack) or to a sensitive attribute (attribute inference/linkage attack) in published data (Samarati 2001, Samarati and Sweeney 1998). The attacker is assumed to know that a user record exists in the published data along with some quasi identifiers[11]. The second category aims at achieving the uninformative principle by randomization mechanisms (Machanavajjhala et al. 2009, Yang et al. 2018) to preserve user privacy against arbitrary adversary knowledge. In our case, since the data collector would have knowledge of what exact data are shared with the privacy attacker, we consider two examples of definitive privacy threats - sensitive attribute inference and re-identification attacks. We formally define these later in the context of location data in Section 4.1.

4. Methodology

Our framework aims at enabling a location data collector to publish data in a privacy preserving manner while ensuring that an advertiser gets sufficient utility. We will introduce the notations first and then define privacy preservation in the context of the location data.

[11] A set of attributes that potentially identify record owners.

Definition 1 (Trajectory)**.** *A trajectory T_i of a user i is defined as a temporally ordered set of tuples $T_i = \{(l_1^i, t_1^i), ..., (l_{n_i}^i, t_{n_i}^i)\}$, where $l_j^i = (x_j^i, y_j^i)$ is a location where x_j^i and y_j^i are the coordinates of the geographic location* [12]*, and t_j^i is the corresponding timestamp, n_i is the number of locations tracked of user i.*

Privacy preservation in the context of location data can be formally stated as—Given a set of N user trajectories $T = \{T_1, ..., T_N\}$, a data collector aims to find a function or a transformation of T, the trajectories to be shared, $T \rightarrow \mathcal{P}(T)$ such that the privacy risk $\mathcal{PR}$ of published trajectories $\mathcal{P}(T)$ is minimized while maintaining the data utility $\mathcal{U}$. We break this down into the following three sub-problems.

Research Question 1 (Risk quantification)**.** ***Given*** *user trajectories T and a privacy threat $\mathcal{PR}$, we aim to* ***find*** *the user-specific risk, $\{r_1, ..., r_N\}$ associated with T. $r_i \in [0, 1]$ would indicate the success rate of an attacker in inferring private information from user i's trajectory T_i.*

Research Question 2 (Utility measurement)**.** ***Given*** *user trajectories T we aim to* ***measure*** *the utility of the trajectories, $\mathcal{U}(T)$, to an advertiser.*

Research Question 3 (Obfuscation scheme)**.** ***Given*** *user trajectories T and their corresponding risk scores, for an advertiser's data utility, $\mathcal{U}(T)$, we aim to* ***find*** *$T \rightarrow \mathcal{P}(T)$, where $\mathcal{P}(T)$ selects a subset of location tuples from each T_i, balancing r_i and utility $\mathcal{U}(T)$.*

We introduce our framework with the three components discussed in Fig. 1 addressing the three sub-problems. In Section 4.1, we detail risk quantification for two classes of privacy threats (RQ 1), in Section 4.2, we introduce our business application and computation of location data utility (RQ 2). Finally, in Section 4.3, we propose an obfuscation scheme that provides a balance between privacy risk and data utility. (RQ 3)

4.1. Risk Quantification

The first step of our framework is quantifying each user's privacy risks. To accomplish this, we simulate a privacy attacker's actions and assign its success in obtaining individual's sensitive information as a user privacy risk. Privacy attacks could range from using simple heuristics, such as querying the user trajectories, to leveraging more robust machine learning heuristics to predict sensitive user attributes (Li et al. 2007, Yang et al. 2018). In our framework, we consider both simple and sophisticated heuristics. Specifically, we will examine two types of most commonly encountered privacy attacks. In the first type, an attacker aims to infer the complete set of locations of an individual T_i from the published trajectories $\mathcal{P}(T) = \{T_1, , T_N\}$, orchestrating an "re-identification attack" (Pellungrini et al. 2018). With some background knowledge, such as a subset of user's locations $\overline{T_i} \in T_i$, an attacker could query the published trajectories $\mathcal{P}(T)$ to identify a subset of users

[12] Co-ordinates usually correspond to a pair of latitude and longitude.

$\overline{T} = \{T_1, , T_r\}, \overline{T_i} \in \overline{T_j}; \forall j \in [1:r], r \leq N$, where $\overline{T}$ consists of all the individuals who have visited the locations in $\overline{T_i}$. The success of the attacker in obtaining T_i would depend on the value of r - lower the value of r, higher the success. Next, exploiting obtained complete individual trajectory, T_i, an attacker could employ a robust machine learning heuristic and extract spatial and temporal information from them to further infer other sensitive information ("sensitive attribute attack") such as home/work address of the user (Yang et al. 2018). In the following sub-sections, we first discuss the information an attacker could extract from published trajectories and then quantify each of these privacy attacks.

4.1.1. Trajectory Feature Extraction ($\mathcal{F}(T)$) Before we assess each user's privacy risks, we extract a set of features from the users' trajectories. To accomplish this, we assume that a subset of those who acquire the data from a data collector, thus having access to the complete set of trajectories, perform privacy attacks. Additionally, from the published trajectories, the attacker could obtain other spatial and temporal information. To replicate the adversarial actions of an attacker, we extract a comprehensive set of features from trajectories[13] studied by the literature (Gonzalez et al. 2008, Eagle and Pentland 2009, Williams et al. 2015, Pappalardo et al. 2016, Ashbrook and Starner 2003, Zheng et al. 2010, Wang et al. 2011). These extracted features, as we will see later in Section 5.3 also help a data collector interpret which features contribute to user risk, gain insights on possible obfuscation schemes, and measure and interpret data utility to advertisers. We categorize the features as,

1. **User Mobility** : This set of features captures the aggregate user mobility patterns based on the locations visited in T_i. We consider the frequency, time spent (Pappalardo et al. 2016), and distance traveled by a user to visit a location (Williams et al. 2015). We also compute other richer mobility features, such as entropy (Eagle and Pentland 2009) and radius of gyration (Gonzalez et al. 2008). A detailed description of these user mobility features is listed in Table 2.

2. **User-Location affinity** : Leveraging the literature on learning significant locations from predicting movement across user trajectories (Ashbrook and Starner 2003, Zheng et al. 2010), we build three user-location tensors: the time spent at each location, frequency of visiting the location, and total distance[14] traveled to the location by a user at a weekly level. Each of these three tensors is of order three—user by unique location by week. We then extract user specific, lower dimensional representations by performing a higher order singular value decomposition (HOSVD) (De Lathauwer et al. 2000) on the three tensors separately. HOSVD is usually applied to extract features from multivariate data with temporal and spatial dimensions similar to ours (Fanaee-T

[13] By definition 3, $\mathcal{P}(T)$ and T are both a set of trajectories and similar features can be extracted from both.

[14] Distance travelled by a user to visit a location is computed from the immediate previous location visited.

and Gama 2015). Since the tensors are populated over the locations that these users have each visited, the extracted features, would effectively capture affinity of the users to significant locations.

3. **User-User Affinity** : Prior studies have also predicted user network or social links based on trajectories (Wang et al. 2011). We thus quantify the users' co-location behavior and build user-user affinity tensors based on locations that the users share at a weekly level. We again populate the tensors with the total weekly time spent, average frequency, and distance traveled to the co-visited locations within a week. These would be third order tensors as well—user by user by week. Next, we perform a HOSVD on the three tensors to extract the user specific low dimensional representations indicative of their affinity to other users. The incremental benefit of the affinity features is discussed in Section 5.

Stylized example: We illustrate the above user-location and user-user affinity features using a stylized example. Consider three user trajectories as defined in Definition 1 —$T_1 = \{(A,1),(B,1),(A,2),(A,2)\}$, $T_2 = \{(C,1),(A,1),(A,1)\}$, $T_3 = \{(D,1),(B,1),(C,2)\}$, where A, B, C, D are location identifiers and the granularity of the timestamps is at a week level. That is, $T = \{T_1, T_2, T_3\}$ reveals that these three users visited four unique locations over a period of two weeks. The three user-location tensors would be of size $[3 \times 4 \times 2]$. The frequency matrix for user corresponding to T_1 is $\begin{pmatrix} 1 & 1 & 0 & 0 \\ 2 & 0 & 0 & 0 \end{pmatrix}$, where the rows and columns correspond to the weeks and unique locations respectively. The three user-user location tensors would be of size $[3 \times 3 \times 2]$ and the frequency matrix for user corresponding to T_i would be $\begin{pmatrix} 1 & \frac{(1+2)}{2} & \frac{(1+1)}{2} \\ 1 & 0 & 0 \end{pmatrix}$ where rows and columns correspond to weeks and users in T. The matrix for user 1's trajectory, T_1, is populated based on the co-visited locations, $(A,1)$ with user 2 and $(B,1)$ with user 3. The time and distance tensors can be similarly built in both cases. We then perform a HOSVD[15] on these tensors separately to extract user specific features. Next, we imitate how an attacker would use the information from the published trajectory data (captured by $\mathcal{F}(T)$) to perform user privacy attacks.

4.1.2. Sensitive Attribute Attack Using the published trajectories $\mathcal{P}(T)$ and the information extracted from them $\mathcal{F}(T)$, an attacker could aim to infer various sensitive attributes, such as age and gender, from the published trajectories $\mathcal{P}(T)$, thus posing a threat to user's privacy. In this type of attacks (Li et al. 2007), the assumption is that an attacker has a model $\mathcal{M}$ to infer the attributes from $\mathcal{P}(T)$ (Yang et al. 2018). Intuitively, the more certain an attacker is about a user's sensitive attribute based on $\mathcal{M}$, the higher is the risk to the user's privacy. To replicate the attacker's actions, we train a supervised model, $\mathcal{M}_{proxy}$ with the features $\mathcal{F}(T)$ extracted from the trajectories. This acts as a proxy for attacker's $\mathcal{M}$ to perform inferences. To quantify each user's

[15] We use the first five principal components of the decomposition. Hence for each user and tensor, we have five lower dimensional representation capturing the user-location and user-user affinity.

Feature	Description
`average_locations`	Number of locations in T_i averaged weekly.
`average_ulocations`	Number of unique locations in T_i averaged weekly.
`average_distance`	Distance travelled by a user to visit locations in T_i, averaged weekly.
`average_dwell`	Time spent at locations in T_i averaged weekly.
`avg_max_distance` (Williams et al. 2015)	Average of the maximum distance travelled by a user each week.
`freq_rog`, `time_rog`, `dist_rog` (Gonzalez et al. 2008)	Radius of gyrations is the characteristic distance traveled by an individual. $rog_i = \sqrt{\frac{1}{\lvert T_i \rvert}\sum_{j=1}^{\lvert T_i \rvert} w_{ij}(l_{ij} - l^i_{cm})^2}$ $l^i_{cm} = \frac{1}{\lvert T_i \rvert}\sum_{j=1}^{j=\lvert T_i \rvert} l_{ij}$, l_{ij} are the geographical coordinates l^i_{cm} is the center of mass of the user w_{ij} are weights obtained based on frequency, time & distance w.r.t to l_{ij}
`freq_entropy`, `time_entropy`, `dist_entropy` (Eagle and Pentland 2009)	Mobility entropy measures the predictability of user trajectory. $E_i = -\sum_{j=1}^{\lvert T_i \rvert} p_{ij} log_2 p_{ij}$, p_{ij} computed from w_{ij} for time, frequency & distance.

Table 2 Description of user mobility features

risk, we assign the certainty of identifying a sensitive attribute from the user's published trajectory data using $\mathcal{M}_{proxy}$.

Proxy attacker model ($\mathcal{M}_{proxy}$) In light of its flexibility of handling regression and classification tasks, and its competitive performance across a wide range of supervised learning algorithms, we use Random Forest (Breiman 2001, Liaw et al. 2002) as $\mathcal{M}_{proxy}$. For each sensitive attribute, we learn a Random Forest, using trajectory features $\mathcal{F}(T)$[16]. The risk associated is then assigned as the certainty of $\mathcal{M}_{proxy}$ in identifying a sensitive attribute. For a classification task, this is the probability of correctly identifying the sensitive attribute. For regression, we assign the negative[17] of the root-mean-square error as the risk[18].

4.1.3. Re-identification Attack Adapting the notion of the risk that a privacy attacker is able to identify a user and associate him/her to a record in published data (Samarati 2001,

[16] We have also compared Random Forest with a number of tree-based and boosting classification methods – xGBoost (Chen and Guestrin 2016), Conditional inference trees (Hothorn et al. 2015), Adaboost (Hastie et al. 2009); and found that Random Forest provided the best out-of-sample performance for our data.

[17] More the error, less certain the attacker is about the sensitive attribute

[18] We perform a 0-1 normalization in case of regression, such that $r_i \in [0, 1]$

Samarati and Sweeney 1998), we define re-identification attack in the context of location data. In this type of threat, an attacker tries to re-identify all the locations visited by a user based on some prior knowledge of an (often small) subset of locations visited by the user. For example, in reality, an advertiser may likely have knowledge about a customer's name, home and work addresses from a membership program registration form. Based on this "background knowledge" of two frequently visited location points, a potential malicious activity would be to link such knowledge to the anonymized location trajectory data and try to re-identify the customer's entire location trajectory associated with the name. Formally, this problem can be defined as follows:

Definition 2. *Given the published trajectory data, $\mathcal{P}(T)$ and a subset of trajectory from user i under attack $\bar{T}_i \subseteq T_i$, $|\bar{T}_i| = k$, the attacker aims to identify T_i from $\mathcal{P}(T)$.*

Notice that a data collector does not know user i under attack or the subset $\bar{T}_i$ a-priori. Hence, to quantify the user risk r_i, one would need to account for all possible $\binom{|T_i|}{k}$ subsets of T_i for all N users. For each such subset, $\bar{T}_i$, the probability of an individual being identified completely (i.e., to infer T_i) is $\frac{1}{N_{T_i}}$, where N_{T_i} denotes number of users in N who have visited the locations in $\bar{T}_i$. If a user has not visited locations in $\bar{T}_i$, then the probability of identification would be zero for the subset considered. We quantify a user' re-identification risk as the maximum of these probabilities over all such subsets.

Stylized example: Let $T_1 = \{(A,1),(B,1),(C,2),(C,2)\}$, $T_2 = \{(A,1),(B,1),(A,2)\}$, $T_3 = \{(A,1),(B,1),(C,2)\}$. Assume $|\bar{T}_i| = 2$; to compute risk for T_1, we consider the subset $\{(A,B),(B,C),(A,C)\}$. Corresponding probabilities of user identification are $\{\frac{1}{3},\frac{1}{2},\frac{1}{2}\}$, risk assigned is $max(\frac{1}{3},\frac{1}{2},\frac{1}{2}) = \frac{1}{2}$

Speed-up heuristic : While the re-identification risk can be exactly computed for a given k, it is computationally inefficient with a complexity of $O(\binom{n_i^{max}}{k} \times N)$ where n_i^{max} is maximum number of unique locations visited by a user. To speed up the computation, we leverage a recent work (Pellungrini et al. 2018) that empirically shows the predictability of the re-identification risk for a given k using mobility features. The main idea is to learn a supervised algorithm (Random Forest regressor in (Pellungrini et al. 2018)) by building a set of mobility features, similar to $\mathcal{F}(T)$ discussed in Section 4.1.1. We adopt this idea by augmenting the mobility features with the user-user and user-location affinity features to learn a similar model. We analytically compute the risks for a subset of the users and then use a trained model to approximate the risk for the rest of the users in our empirical study. We will detail this and justify our model choices in Section A.

This completes assignment of risk $\{r_1,...,r_N\}$, $r_i \in [0,1]$ for a given set of trajectories T, under the above two types of privacy threats $\mathcal{PR}$ as defined in RQ 1.

4.2. Location Data Utility

Having quantified the user risks associated with two commonly encountered, definitive privacy threats on location data, we next examine the utility that an advertiser would derive from published trajectories. The behaviorally rich nature of location data enables advertisers to derive insights and perform various targeted marketing activities leading to monetary benefits. In this work, we consider a popular business use case for an advertiser - POI recommendations (Ashbrook and Starner 2003). The underlying idea is to leverage historical user preferences revealed in user trajectories to predict locations that a user is most likely to visit in the future. Predicting a user's future locations accurately would enable an advertiser to target him/her with relevant, contextualized marketing campaigns (Ghose et al. 2018). To this end, we quantify an advertiser's utility in the context of POI-based targeting by learning a recommender model. Intuitively, more accurate POI predictions will render better targeting with the learned recommendation model, leading to a higher utility for the advertiser. Hence, we quantify the data utility as the accuracy of the future predictions made by the recommendation model. Next, we discuss the POI model in more detail.

4.2.1. POI Recommendation Model Most recommendation models focus on the collaborative filtering process—identifying other users with similar historical preferences to infer a user's future preferences (Bobadilla et al. 2011). This is consistent with human social behavior—people tend to consider their acquaitances' tastes, opinions, and experiences when making their own decisions. We thus imitate an advertiser's leverage of the location data for POI-based targeting and compare a number of recommendation models in the literature (comparison in Appendix A). We focus our discussion on the best-performing nearest neighborhood-based (NN) learning technique. Simply put, the main idea in NN is to identify the m users most similar to an individual (namely m neighbors) and utilize their locations to predict the focal individuals future preferences. The similarity is computed based on the visited locations that reveal each user's preferences. The set of features extracted from the user trajectories in Section 4.1.1 $\mathcal{F}(T)$ serves this purpose. And to find the m most similar users, we compute the cosine similarity between two users i, j with trajectories T_i, T_j represented by features $\mathcal{F}(T_i), \mathcal{F}(T_j)$

$$sim(\mathcal{F}(T_i), \mathcal{F}(T_j)) = \frac{\mathcal{F}(T_i) \cdot \mathcal{F}(T_j)}{||\mathcal{F}(T_i)||||\mathcal{F}(T_j)||} \tag{1}$$

After identifying the m most similar users for an individual i, denoted by M_i, we aggregate and rank the locations visited by M_i based on a combination of visit frequency and their similarity to individual i. For each user $j \in M_i$, location $l \in T_j$, let f_j^l denote the number of times the user j visited location l, the rank of a location l for a user j is determined by the following quantity

$$r_{ij}^l = \sum_{l=1}^{|T_j|} \frac{f_j^l}{\sum_l f_j^l} sim(\mathcal{F}(T_i), \mathcal{F}(T_j)) \tag{2}$$

In the above equation, $\frac{f_j^l}{\sum_l f_j^l}$ is the normalized frequency of visits at a user level for a location. Intuitively, Equation 2 ensures that an individual i is most likely to visit the most frequently visited location of the most similar user. We further aggregate r_{ij}^l across all the users who visited the location l in M_i by computing the mean of r_{ij}^l , that is

$$r_i^l = \frac{1}{\sum_{j=1}^{|M_i|} 1(l \in T_j)} \sum_{j=1}^{|M_i|} 1(l \in T_j) \cdot r_j^l \tag{3}$$

where $1(j \in T_j)$= 1 if user j has visited location l and zero otherwise. Higher the value of r_i^l, more likely that an individual i visits location l in the future. The next k locations an individual i is most likely to visit correspond to the top k ranked locations in M_i. The utility of an advertiser is measured as the accuracy of the predictions made by the recommender for the different values of k. This is computed by the widely used information retrieval metrics that assess the quality of the recommendations - Mean Average Precision at k ($MAP@k$), Mean Average Recall at k ($MAR@k$) (Yang et al. 2018). $MAP@k$ and $MAR@k$ are calculated by first computing the average precision for the k predictions made for each user i, and then averaging across all users.

More specifically, let $L_i = \{l_i^1, l_i^2, , l_i^{k'}\}$ be the true temporally ordered locations that a user has visited in the future and $\overline{L_i} = \{\overline{l_i^1}, \overline{l_i^2}, ..., \overline{l_i^k}\}$ be the predictions made by the NN recommender ordered by the ranks based on Equation 3. First, the average precision AP_i^k and average recall AR_i^k for user i with top k recommended locations are given by

$$AP_i^k = \frac{1}{|L_i \cap \overline{L}_i|)} \sum_{j=1}^{k} \frac{|L_{1:j} \cap \overline{L}_{1:j}|}{|L_{1:j}|)} \tag{4}$$

$$AR_i^k = \frac{1}{|L_i \cap \overline{L}_i|)} \sum_{j=1}^{k} \frac{|L_{1:j} \cap \overline{L}_{1:j}|}{|L_i|)} \tag{5}$$

The intuition is that AP_i^k measures the proportion of the recommended locations that are relevant, while AR_i^k measures the proportion of relevant locations that are recommended. Then, $MAP@k$ and $MAR@k$ are computed by averaging AP_i^k and AR_i^k across all the users. The parameter m, number of the most similar neighbors used for location predictions, is selected by performing a five-fold cross-validation[19] aimed at maximizing the accuracy of the recommendations. We will detail how we have selected the number of the most similar neighbors in our empirical setting in Section 5.1.2.

[19] This is a technique commonly used in statistical learning literature to ensure a good out-of-sample performance (Friedman et al. 2001)

4.3. Obfuscation Scheme

The last step in our framework is to address RQ 3 – devising an obfuscation scheme that would balance the privacy risks and utilities of the published trajectories to advertisers. Given the unique properties of the location data of high dimensionality (due to the large number of locations visited by the users), sparsity (fewer overlap across the locations visited by the users) and sequentiality (the temporal order of the visited locations by users), employing the traditional obfuscation techniques proposed for relational data, such as k-anonymity (Samarati and Sweeney 1998), ℓ-diversity (Machanavajjhala et al. 2006), and confidence-bounding (Wang et al. 2007) would be computationally prohibitive and significantly reduce the utilities of the resulting obfuscated data (Aggarwal 2005).

On the other hand, those techniques devised specifically for trajectory data are often complex for a data collector to interpret and apply in practice. For instance, the $(K, C)_L$ privacy framework (Chen et al. 2013), an anonymization scheme built on the principles of k-anonymity requires multiple parameter inputs from a data collector. The parameters may include the threshold of the attacker's success probability, or the attacker's background knowledge in each type of threat. For instance, LSup (Terrovitis et al. 2017) that suppresses the trajectories by quantifying the trade-off between the utility to advertisers and the risks associated with each location visited by a user requires similar inputs. Given the complex nature of such heuristics, setting these parameters and interpreting the resulting obfuscations for practical purposes is non-trivial. Further, the current techniques do not provide the flexibility for a data collector to make a choice between multiple obfuscation schemes.

Addressing these critical challenges, we develop $\mathcal{P} : T \rightarrow T$, a personalized user-specific suppression technique that is interpretable to the data collector since it requires merely a single parameter input that corresponds to a re-identification attacker's background knowledge – the cardinality of the set $\overline{T_i}$ as defined in Definition 2. Intuitively, this means that our method requires only one parameter input regarding the number of a user's locations already known to the attacker (and thus used as the background knowledge to re-identify the user's full trajectory). In addition, the suppression technique requires no input parameters for the sensitive attribute attack. Furthermore, we will offer the data collector the flexibility to choose across multiple, interpretable obfuscations for each type of privacy attack.

4.3.1. Personalized Data Suppression ($\mathcal{P}$) The main idea of our obfuscation scheme is to suppress each user's information proportionally based on the corresponding user-level privacy risk computed in Section 4.1. By incorporating each individual user's risk r_i, in $\mathcal{P}$, we ensure the reduction of the specific user's risk in the published trajectories – one of the aims of privacy-preserving data sharing. We achieve this by introducing a decision parameter $p \in [0, 1]$, and define

a user-specific suppression score $z_i = r_i \times p$, $z_i \in [0,1]$ since $r_i, p \in [0,1]$. The number of locations in $\mathcal{P}(T_i)$ published for a user is then controlled by z_i. Also, each location tuple in T_i is independently[20] suppressed with probability z_i.

Intuitively, for a value of p, users at higher risk have more locations suppressed in their published trajectories compared to lower risk users. This information loss due to the suppression would adversely affect the ability of an attacker to perform attacks as well as an advertiser's utility from $\mathcal{P}(T)$. For instance, in the extreme scenario $p=1$ and all user risks $r_i=1$ (complete suppression), all locations would be suppressed, $\{\mathcal{P}(T_i)\} = \mathcal{P}(T) = \emptyset$ resulting in no utility to the advertiser or threat to user privacy. A similar inference can be made when $p=0$ (no suppression) when $\{\mathcal{P}(T_i)\} = \mathcal{P}(T) = T$ resulting in the maximum data utility and privacy risk. Noting these two extreme scenarios, we empirically determine the value of p and the corresponding $\mathcal{P}(T)$ that provides a utility-risk balance accounting for both risks detailed in Section 4.1.

Our obfuscation scheme has two main advantages. First, introducing the decision parameter p while performing the user-level suppression provides a data collector with multiple trade-off choices. Second, the user-specific suppression scores z_i provides individual level interpretability of the obfuscation mechanism to a data collector. Measurement of the utility of the published trajectories $\mathcal{P}(T)$ follows the approach discussed in Section 4.2 using the information retrieval metrics that assess the quality of the recommendations - Mean Average Precision at k ($MAP@k$), Mean Average Recall at k ($MAR@k$) where k denotes top k ranked recommended locations based on user's historical preferences (Yang et al. 2018). The individual privacy risks (Section 4.1) for $T_i \in \mathcal{P}(T)$ are computed for the above two privacy threats. The mean of each individual's risks is estimated to be the aggregated privacy risk associated with $\mathcal{P}(T)$. By fine-tuning the decision parameter p, our final goal is to understand, measure, and optimize the trade-off between data utility ($\mathcal{U}$) and privacy risk ($\mathcal{PR}$) in a meaningful way.

5. Results

5.1. Empirical Setup

An overview of our empirical setup is presented in Figure. 1 Our obfuscation scheme is dependent on the decision parameter $p \in [0,1]$. In our empirical study, we vary $p \in \mathcal{G}_p = \{0, 0.1, ..., 1\}$ to compute the quantities that reflect the overall data utility ($MAP@k$, $MAR@k$) and privacy risk for each p.

5.1.1. Risk Computation First, we estimate the overall user risk for various levels of obfuscations ($p \in \mathcal{G}_p$). For each type of threat , we first quantify the user-level risk by extracting features $\mathcal{F}(T)$ for the entire sample ($p=0$) without any obfuscation. These risks are baseline individual

[20] As we will see in our empirical study Section 5, we estimate three risk scores associated with the privacy attacks. The suppression is performed independently for each of them.

risks when the location data are stored or shared as is (Part A in Figure 1). Based on these baseline risks, we perform user-level obfuscation by varying $p \in \mathcal{G}_p$ (Part B in Figure 1). We then repeat the process – extracting features and re-calculating the user risks on each obfuscated trajectory sample $\mathcal{P}(T)$. Finally, we compute the overall privacy risk by averaging the risks across all users. To obtain a consistent estimate, we use bootstrapping with 20 trials for each $p \in \mathcal{G}_p$.

In the sensitive attribute attack , we consider two sensitive attributes - home address and mobile operating system predictions from the original trajectory data. To train the predictive model, we assume, consistent with the literature, that an attacker has access to the sensitive attributes of a subset of users, such as via surveys (Yang et al. 2018, du Pin Calmon and Fawaz 2012). This assumption is as if the attacker has access to a training sample with known trajectories and sensitive attributes, thus capable of inferring sensitive attributes from new trajectories.

To simulate this process, we split the data into two random samples: 50% training set (T_{train}) with 20,000 users, and 50% test set (T_{test}) with 20,012 users. We use T_{train} to train the predictive model for the privacy risk. Recall that in our risk quantification (Section 4.1), we use Random Forest regressor to predict the risks of home locations and use Random Forest classifier to predict mobile operating system and re-identification risks. To avoid over-fitting, we perform a five-fold cross-validation on T_{train} and pick two optimal hyper-parameters specific to the Random Forest – the maximum number of features in the tree and the number of trees (see the Appendix A for more details). Cross-validation ensures that the model produces better out-of-sample predictions (Friedman et al. 2001). Once the model is trained, we apply it to estimate the risk in each privacy threat on T_{test}. In Figure 3, we report the mean of these risks computed for each p across all 20,012 users in T_{test}.

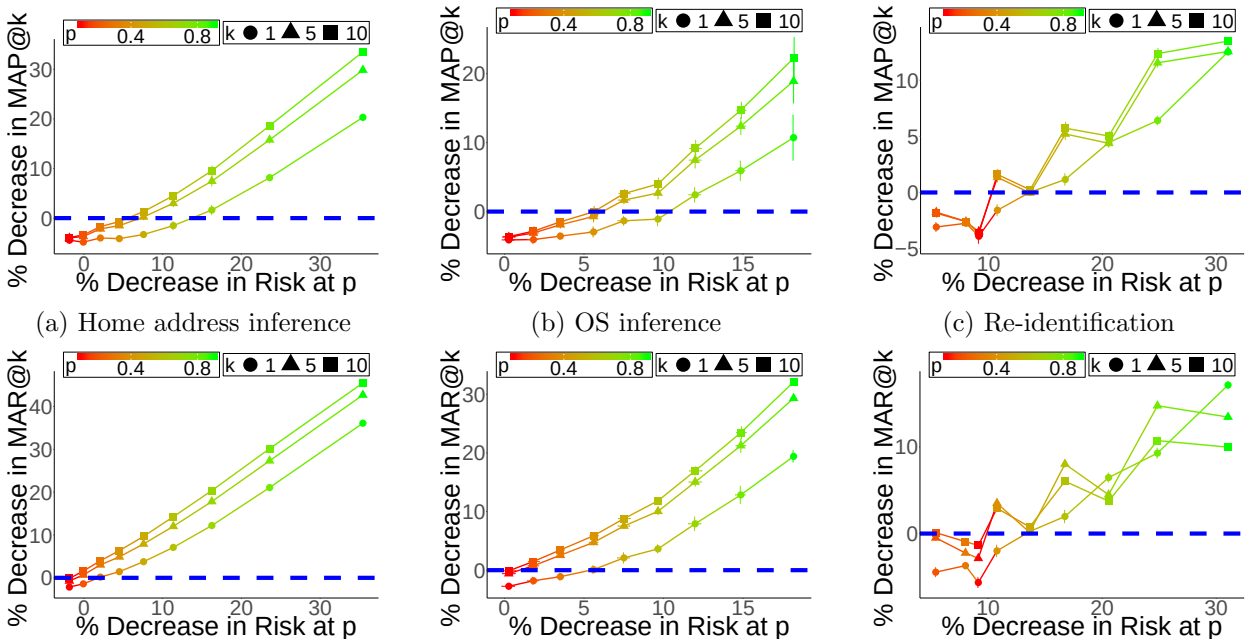
To compute the privacy risk of re-identification attack, we need to know the number of locations in each user's trajectory that a privacy attacker has already known. In our empirical study, we assume this number to be 2 and hence set $|\bar{T}_i| = 2$ in Definition 2.[21]

5.1.2. Utility Measurement Next, we compute the data utility under different obfuscations. To do so, we compute the performance of a neighborhood-based collaborative filtering recommendation heuristic to accurately predict future user locations. To assess the predictive accuracy, we treat the locations actually visited by each user in the fifth week as the ground truth and train the recommender model to predict these locations.

Based on the user risks, we perform varying levels of obfuscation, $p \in \mathcal{G}_p$. We learn a neighborhood-based recommender (Bobadilla et al. 2011) that tunes the number of neighbors via a five-fold cross-validation on the obfuscated data. The model is learned to rank the locations that

[21] We make this assumption for our empirical study. The model learning is generalizable for other values of $|\bar{T}_i|$.

a user is likely to visit in the fifth week of the observation period. That is, we build the features (discussed in Section. 4.1.1) on the first four weeks of the obfuscated data and tune the number of neighbors[22] to maximize the prediction accuracy. Then, we compute the utility —$MAP@k$, $MAR@k$ for $k = \{1, 5, 10\}$[23]. Intuitively, $MAP@1$ and $MAR@1$, for example, represent an advertiser's utility to predict the next location that a user is most likely to visit in the fifth week based of the recommender model learned on the obfuscated data. Similar to what we have done for the risk metrics, we perform 20 trials for each p and report the mean and 95% confidence intervals of the utility metrics (Figure 3). A more detailed explanation of the utility computation is available in the Appendix B.



(a) Home address inference (b) OS inference (c) Re-identification

(d) Home address inference (e) OS inference (f) Re-identification

Figure 3 Proposed framework - $MAP@k$ and $MAR@k$ for varying p

5.2. Privacy-preserving Obfuscation

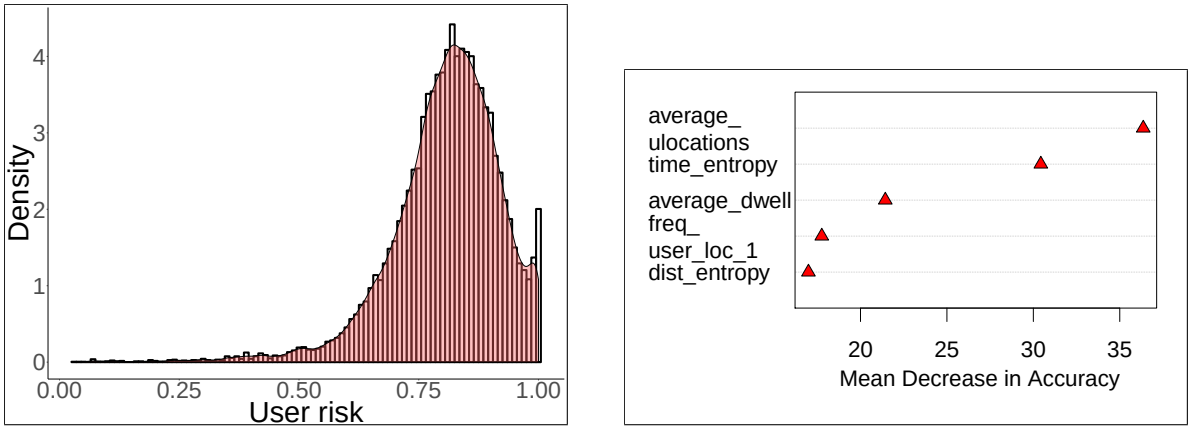
In Figures 3a, 3b, 3c we visualize the trade-off between data utility and privacy risk. The X and Y axes display the percentage decrease in the aggregate risk and $MAP@k$ from the original sample ($p = 0$) with no obfuscation for each $p \in \mathcal{G}_p$ respectively. We plot these for $k = \{1, 5, 10\}$. Intuitively, the higher the value of X-axis, the more the decrease in the overall risk and hence better preservation of privacy. On the other hand, the lower values of Y-axis correspond to a lesser decrease in the utility

[22] We use the following grid for number of neighbors - $\{5, 10, 25, 50, 100, 200\}$

[23] The learned recommender model can be used to compute $MAP@k$, $MAR@k$ for other values of k as well. We consider $k = \{1, 5, 10\}$ to illustrate the method's efficacy.

of the obfuscated data compared to the original data, suggesting a similar utility for the advertiser even after obfuscation. A data collector who aims to trade off between utility and privacy, is thus presented with multiple choices in our framework. Ideally, a good choice for obfuscation would be the values of p that correspond to a higher value along the X-axis and a lower value along the Y-axis. In the figures, the horizontal blue line, with no decrease in data utility from obfuscation indicates these choices. Similar insights can be drawn from figures 3d, 3e, 3f where we compare the percentage decreases in $MAR@k$ to the percentage decreases in the aggregate risk.

In all the figures in Figure 3, we observe that as we increase p, both the quantities decrease in aggregate risk (X-axis) and decrease in performance measures (Y-axis) increase. This is expected since an increase in p, for the same user risk scores, more locations get suppressed, meaning more information loss to an advertiser's utility as well as a privacy attack. For a given percentage decrease in risk, we observe a lesser corresponding percentage decrease in performance. This can be explained by the framework's obfuscation scheme that is based on user risk scores that capture the success of a privacy attack. This risk-based obfuscation would penalize and cause more information loss to the attacker's adversarial intent compared to the utility. The figures also emphasize the proposed framework's flexibility to provide a data collector with several interpretable choices for obfuscation. Further, since our obfuscation scheme works by suppressing a set of location tuples instead of randomization (Yang et al. 2018) or splitting (Terrovitis et al. 2017), this would also have potential benefits to the server costs incurred by an advertiser in storing and analyzing the location data.



(a) User risk density plot - OS inference threat (b) Feature importance, OS inference model

Figure 4 Personalized Risk Management Insights

5.3. Personalized Risk Management

Here, we discuss insights a data collector can gain from the risk quantification we perform for different types of threats prior to obfuscation. In Section 4.1 we extract a comprehensive set of features ($\mathcal{F}(T)$) and then build predictive models to assess user privacy risk associated with two specific privacy threats—sensitive attribute (individual home address and operating system) and re-identification attacks. In Figure 4a, we visualize the density plot of user risk on non-obfuscated trajectory data. The user risks were computed by mimicking an attacker's aim to infer the operating system of a user. A data collector, by looking at Figure 4a can have a precise estimation of the distribution of user privacy risk. For example, a majority of users have a relatively high risk ($\geq$ 0.75) of their sensitive attribute being inferred if there was no obfuscation performed.

Similarly, we find that in the case of home address inference, the average estimated user risk is 0.84. By assessing the error of the Random Forest regressor learned to predict the home address, we observe that an attacker on average could successfully identify a consumer's home address within a radius of 3,900 metres $\approx$ 2.5 miles (Discussed in more detail in Appendix A). Further, the average risk of re-identifying an individual's entire trajectory by knowing only two randomly sampled locations is 0.49, meaning a 49% chance of success for a privacy attacker.

These privacy risks associated with non-obfuscated data can be curtailed by a data collector by using our framework's obfuscation scheme. For instance, the risk associated with operating system inference could be bought down by 10% (Refer to Figures 3b, 3e $p = 0.6$) while still being able to fully preserve the data utility with regard to the POI@1 performance. As a follow-up step, by implementing the POI recommendation strategy in the real world, a data collector can also measure the monetary value of an individual trajectory, and compare it with the user-specific privacy risk to better understand customer lifetime value (Berger and Nasr 1998) and personalize customer relationship management.

In addition, prior to obfuscation, a data collector could look at feature importance in our model. In Figure 4b we visualize the top five important features of the Random Forest we train to compute user risks we plot in Figure 3b. From the figure, a data collector can infer that temporal information of the trajectories (`time_entropy`, `average_dwell`) contributes significantly to model predictive performance. Hence, a possible obfuscation scheme that removes the timestamps (even partially) in the trajectories preventing the attacker to construct the temporal features could reduce the user risk considerably. Similar insights can be gained by analyzing the risk scores related to other privacy attacks.

5.4. Model Comparisons

We compare our framework's obfuscation scheme with two kinds of baselines – rules derived from timestamps of user locations and alternate suppression schemes based on user risk.

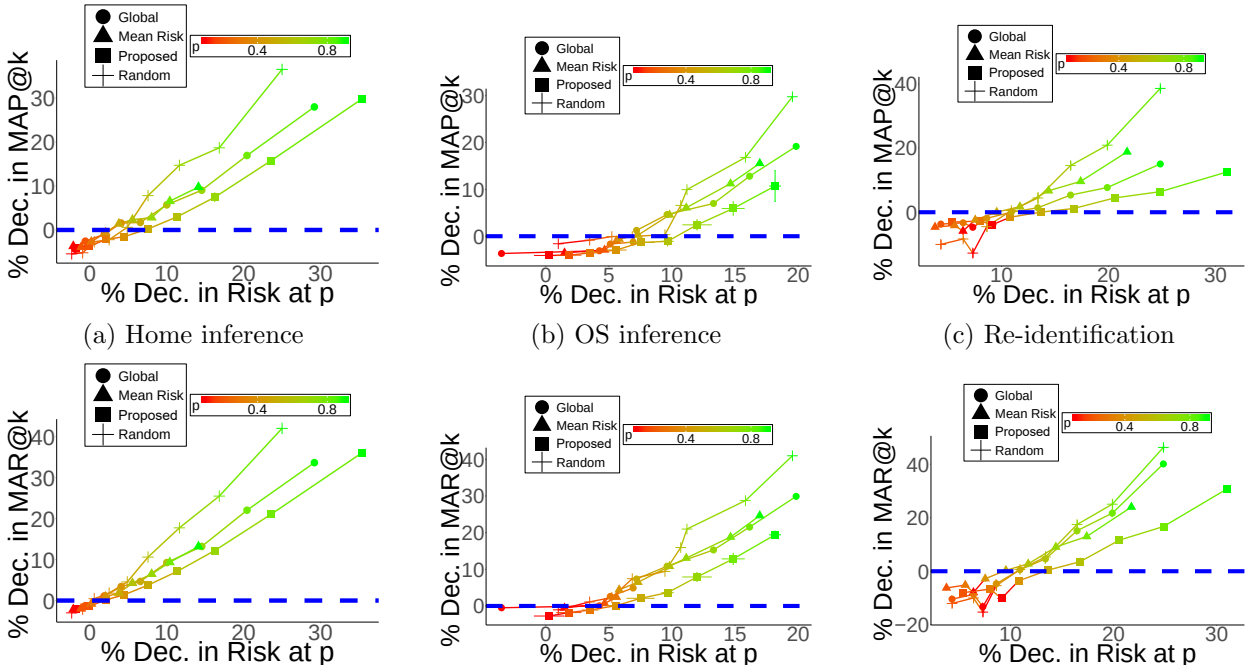
Obfuscation rule	% Decrease Home address risk	% Decrease Operating system risk	% Decrease Re-identification risk	% Decrease Utility (MAP@1)	% Decrease Utility (MAR@1)
Remove Sleep hours	2.43	12.51	1.41	11.83	12.69
Remove Sleep and working hours	10.72	21.84	21.49	34.45	23.72
Remove time stamps	13.45	25.49	0	33.16	32.97

Table 3 Alternative Schemes: Rule-based Obfuscation

5.4.1. Comparison to Rule-based Obfuscations: We derive a few practical rules for obfuscation based on the timestamps of user locations in the location data. In the absence of a privacy-friendly framework, a data collector could perform obfuscation by choosing to 1) Remove all the locations during the usual sleeping hours (10 PM - 7 AM) on all days, 2) Remove locations in sleeping hours and working hours (9 AM - 6 PM) on weekdays, or 3) Remove timestamps of locations entirely before sharing the data. The three time-based rule obfuscations would reduce the amount of information that can be extracted from the shared location data and hence would adversely affect the advertiser's utility and adversarial intent to invade consumer's privacy. For instance, if the timestamps of the location data were to be removed both mobility features (refer Table 2) – `time_entropy`, `time_rog`, `average_dwell` and the User-User, User-Location affinity features (refer Section 4.1.1 based on time spent by a user at a location cannot be computed.

The decrease in risks for the two threats and decrease in utility for each of these obfuscations are presented in Table 3. As expected, there is a decrease in both risk and utility. In the home address inference attack (Figure 3a, $p = 0.7$, $k = 1$), we find that a risk to user privacy can be reduced by 15% (maximum decrease when compared to rule-based heuristics) with less than 1% decrease in MAP@1 (minimum decrease). A similar trend is observed in re-identification attack (Figures 3c, 3f). In the operating system inference (Figure 3a, $p = 0.9$, $k = 1$), we observe that risk is reduced by $\approx$ 18% compared to 25.49% when timestamps are removed. However, this is achieved with a lesser decrease in utility $\approx$10% using the proposed framework when compared to the 33%. Overall, we find a better choice set for the trade-off justifying a need for a privacy-friendly framework to assist a data collector to share location data in a privacy-friendly way.

5.4.2. Comparison to Risk-based Obfuscations We compare the proposed obfuscation framework to three alternate suppression baselines. These are devised to show the efficacy of user risk quantification and personalized local suppression of trajectories performed in our framework.



(a) Home inference (b) OS inference (c) Re-identification

(d) Home inference (e) OS inference (f) Re-identification

Figure 5 **Proposed framework vs risk-based obfuscations** - $MAP@1$ **and** $MAR@1$

1. **Random** - In this baseline, we do not perform suppression of locations at a user level. Instead of hiding location tuples in T_i based on $z_i = r_i \times p$, we randomly suppress locations in T. We suppress the same number of location tuples as in our framework's obfuscation scheme to make it comparable.

2. **Mean Risk** - Here, we perform a user-specific suppression without any variation across users here. We replace the user risk score r_i with the mean $\bar{r} = \frac{1}{N}\sum_i r_i$ as r_i and hide locations using $z = \bar{r} \times p$ for each T_i.

3. **Global** - In this baseline, we suppress a location tuple globally. That is, a tuple in any T has the same chance of being suppressed irrespective of a different user risk threat. This is different from our obfuscation scheme where a tuple may not be suppressed for a less risky but has been suppressed for a high risk user. For each tuple, we assign the mean of user risk scores as tuple risk score, vary p and perform suppression.

We empirically compare the proposed obfuscation scheme to the baselines listed and visualize $MAP@1$ and $MAR@1$ in Figure 5. We observe that, for a given decrease in risk, our framework's obfuscation has the least decrease in utility gain across all three threats. Random baseline, which is an ablation of our obfuscation scheme without the risk quantification step performs the worst among competing models. This justifies a need for threat quantification either at a user-level (Mean Risk and proposed obfuscation) or at a location tuple level (Global). Better performance than Mean Risk baseline shows that a personalized level of obfuscation for each user is necessary. Finally,

a higher utility gain over Global baseline emphasizes the need for quantifying and suppressing locations at a user level compared to a tuple level.

6. Conclusion

Smartphone location tracking has created a wide range of opportunities for data collectors to monetize location data (Valentino-Devries et al. 2018). Leveraging the behavior-rich location data for targeting is proven to be an effective mobile marketing strategy to increase advertisers' revenues (Ghose et al. 2018). However, these monetary gains come at the cost of potential invasion of consumer privacy. In this research, we tackle this important and under-studied topic from a data collector's perspective. We identify the key challenges faced by a data collector and propose an end-to-end framework to enable a data collector to leverage location data while preserving consumer privacy.

The existing literature on privacy preservation, primarily from the Computer Science discipline, are either unsuited for this new type of data with distinct challenges, or not interpretable or personalized to an individual level. Our research fills this gap. Specifically, we propose a framework of three components, each addressing a key topic facing a data collector. First, we quantify each consumer's risks, exemplified by two common types of privacy attacks – sensitive attribute attack and re-identification attack. These risks are intuitively modeled as the attacker's success probabilities in inferring the consumer's private information. Second, we measure the utility of the location trajectory data to an advertiser by considering a popular business use case - POI recommendations. The utility is estimated by the accuracy of using the location data to infer a consumer's future locations. Finally, to enable a data collector to trade off between consumer risk and advertiser utility, we propose an obfuscation scheme suppressing consumers' trajectories based on their individual risks associated with each privacy attack. The proposed obfuscation scheme provides multiple options for the data collector to choose from based on specific business contexts.

We validate the proposed framework on a unique data set containing nearly a million mobile locations tracked from over 40,000 individuals over a period of five weeks in 2018. To our best knowledge, this research reflects an initial effort to analyze such a rich, granular, newly available human trajectory data; and for the purpose of privacy preservation. We find that there exists a high risk of invasion of privacy in the location data if a data collector does not obfuscate the data. On average, a privacy attacker could accurately predict an individuals home address within a radius of 2.5 miles and mobile operating system with an 82% success. The proposed risk quantification enables a data collector to identify high risk individuals and those features contributing to the risk associated with each privacy attack. Furthermore, using the proposed obfuscation scheme, a data collector can achieve better trade-off between consumer privacy and advertiser utility when

compared to several alternative rule-based and risk-based obfuscations. For instance, in the attack of home address inference, we find that a risk to user privacy can be reduced by 15%, a maximum decrease when compared to rule-based heuristics, with less than 1% decrease in utility, a minimum decrease. In summary, this study presents conceptual, managerial, and methodological contributions to the literature and business practice, as summarized in the Introduction. Besides offering a powerful tool to data collectors to preserve consumer privacy while maintaining the usability of the increasingly accessible form of rich and highly valuable location data, this research also informs the ongoing debate of consumer privacy and data sharing regulations.

Despite the contributions, there are limitations of this research, thus calling for continued explorations of this rich and promising domain. For example, our data contain device IDs, but no detailed demographics, associated with each individual. When such data become available, one may, for instance, develop deeper insights into which demographic sub-populations are most vulnerable to privacy risks. Also, our analysis considered the locations' longitudes and latitudes, but not names (such as Starbucks) or types (such as hospital). Hence future research may further distinguish varied sensitivity levels across locations in privacy preservation. Furthermore, as other data, such as the same individuals' online clickstreams or social media comments, become linked to their mobile location data, more sophisticated privacy preservation methodologies may be developed.

References

Osman Abul, Francesco Bonchi, and Mirco Nanni. Never walk alone: Uncertainty for anonymity in moving objects databases. In *Data Engineering, 2008. ICDE 2008. IEEE 24th International Conference on*, pages 376–385. Ieee, 2008.

Alessandro Acquisti, Leslie K John, and George Loewenstein. The impact of relative standards on the propensity to disclose. *Journal of Marketing Research*, 49(2):160–174, 2012.

Idris Adjerid, Eyal Peer, and Alessandro Acquisti. Beyond the privacy paradox: Objective versus relative risk in privacy decision making. *Available at SSRN 2765097*, 2016.

Idris Adjerid, Alessandro Acquisti, and George Loewenstein. Choice architecture, framing, and cascaded privacy choices. *Management Science*, 2018.

Charu C Aggarwal. On k-anonymity and the curse of dimensionality. In *Proceedings of the 31st international conference on Very large data bases*, pages 901–909. VLDB Endowment, 2005.

Michelle Andrews, Xueming Luo, Zheng Fang, and Anindya Ghose. Mobile ad effectiveness: Hyper-contextual targeting with crowdedness. *Marketing Science*, 35(2):218–233, 2016.

Apple. Apple Has Quietly Started Tracking iPhone Users Again, And Its Tricky To Opt Out, 2012. `http://www.businessinsider.com/ifa-apples-iphone-tracking-in-ios-6-2012-10`, 2012.

Apple. Requesting Permission. `https://developer.apple.com/design/human-interface-guidelines/ios/app-architecture/requesting-permission/`, 2014.

Apple. iOS 10 to Feature Stronger Limit Ad Tracking Control, 2016. `https://fpf.org/2016/08/02/ios-10-feature-stronger-limit-ad-tracking/`, 2016.

Daniel Ashbrook and Thad Starner. Using gps to learn significant locations and predict movement across multiple users. *Personal and Ubiquitous computing*, 7(5):275–286, 2003.

Yakov Bart, Venkatesh Shankar, Fareena Sultan, and Glen L Urban. Are the drivers and role of online trust the same for all web sites and consumers? a large-scale exploratory empirical study. *Journal of marketing*, 69(4):133–152, 2005.

Roberto J Bayardo and Rakesh Agrawal. Data privacy through optimal k-anonymization. In *null*, pages 217–228. IEEE, 2005.

Paul D Berger and Nada I Nasr. Customer lifetime value: Marketing models and applications. *Journal of interactive marketing*, 12(1):17–30, 1998.

Jesus Bobadilla, Antonio Hernando, Fernando Ortega, and Jesus Bernal. A framework for collaborative filtering recommender systems. *Expert Systems with Applications*, 38(12):14609–14623, 2011.

Leo Breiman. Random forests. *Machine learning*, 45(1):5–32, 2001.

Gordon C Bruner and Anand Kumar. Attitude toward location-based advertising. *Journal of interactive advertising*, 7(2):3–15, 2007.

Gordon Burtch, Anindya Ghose, and Sunil Wattal. The hidden cost of accommodating crowdfunder privacy preferences: a randomized field experiment. *Management Science*, 61(5):949–962, 2015.

Ramon Casadesus-Masanell and Andres Hervas-Drane. Competing with privacy. *Management Science*, 61 (1):229–246, 2015.

Ramnath K Chellappa and Shivendu Shivendu. Mechanism design for free but no free disposal services: The economics of personalization under privacy concerns. *Management Science*, 56(10):1766–1780, 2010.

Rui Chen, Benjamin CM Fung, Noman Mohammed, Bipin C Desai, and Ke Wang. Privacy-preserving trajectory data publishing by local suppression. *Information Sciences*, 231:83–97, 2013.

Tianqi Chen and Carlos Guestrin. Xgboost: A scalable tree boosting system. In *Proceedings of the 22nd acm sigkdd international conference on knowledge discovery and data mining*, pages 785–794. ACM, 2016.

Vincent Conitzer, Curtis R Taylor, and Liad Wagman. Hide and seek: Costly consumer privacy in a market with repeat purchases. *Marketing Science*, 31(2):277–292, 2012.

Martijn G De Jong, Rik Pieters, and Jean-Paul Fox. Reducing social desirability bias through item randomized response: An application to measure underreported desires. *Journal of Marketing Research*, 47(1): 14–27, 2010.

Lieven De Lathauwer, Bart De Moor, and Joos Vandewalle. A multilinear singular value decomposition. *SIAM journal on Matrix Analysis and Applications*, 21(4):1253–1278, 2000.

Flávio du Pin Calmon and Nadia Fawaz. Privacy against statistical inference. In *Communication, Control, and Computing (Allerton), 2012 50th Annual Allerton Conference on*, pages 1401–1408. IEEE, 2012.

Jean-Pierre Dubé, Zheng Fang, Nathan Fong, and Xueming Luo. Competitive price targeting with smartphone coupons. *Marketing Science*, 36(6):944–975, 2017.

Cynthia Dwork and Jing Lei. Differential privacy and robust statistics. In *Proceedings of the forty-first annual ACM symposium on Theory of computing*, pages 371–380. ACM, 2009.

Nathan Eagle and Alex Sandy Pentland. Eigenbehaviors: Identifying structure in routine. *Behavioral Ecology and Sociobiology*, 63(7):1057–1066, 2009.

eMarketer. US Smartphone OS Race Still Close, as Men, Younger Users Favor Android. `https://www.emarketer.com/article.aspx?R=1009961&RewroteTitle=1`, 2013.

Hadi Fanaee-T and João Gama. Eigenevent: An algorithm for event detection from complex data streams in syndromic surveillance. *Intelligent Data Analysis*, 19(3):597–616, 2015.

Zheng Fang, Bin Gu, Xueming Luo, and Yunjie Xu. Contemporaneous and delayed sales impact of location-based mobile promotions. *Information Systems Research*, 26(3):552–564, 2015.

Nathan M Fong, Zheng Fang, and Xueming Luo. Geo-conquesting: Competitive locational targeting of mobile promotions. *Journal of Marketing Research*, 52(5):726–735, 2015a.

Nathan M Fong, Zheng Fang, and Xueming Luo. Real-time mobile geo-conquesting promotions. *Journal of Marketing Research*, 2015b.

Jerome Friedman, Trevor Hastie, and Robert Tibshirani. *The elements of statistical learning*, volume 1. Springer series in statistics New York, 2001.

Benjamin C. M. Fung, Ke Wang, Rui Chen, and Philip S. Yu. Privacy-preserving data publishing: A survey of recent developments. *ACM Comput. Surv.*, 42(4):14:1–14:53, June 2010. ISSN 0360-0300. doi: 10.1145/1749603.1749605. URL `http://doi.acm.org/10.1145/1749603.1749605`.

Pedro M Gardete and Yakov Bart. Tailored cheap talk: The effects of privacy policy on ad content and market outcomes. *Marketing Science*, 37(5):733–752, 2018.

Robert Garfinkel, Ram Gopal, and Paulo Goes. Privacy protection of binary confidential data against deterministic, stochastic, and insider threat. *Management Science*, 48(6):749–764, 2002.

Anindya Ghose, Beibei Li, and Siyuan Liu. Mobile targeting using customer trajectory patterns. *Management Science*, Forthcoming, 2018.

Khim-Yong Goh, Kai-Lung Hui, and Ivan PL Png. Privacy and marketing externalities: Evidence from do not call. *Management Science*, 61(12):2982–3000, 2015.

Avi Goldfarb and Catherine Tucker. Online display advertising: Targeting and obtrusiveness. *Marketing Science*, 30(3):389–404, 2011a.

Avi Goldfarb and Catherine Tucker. Rejoinderimplications of online display advertising: Targeting and obtrusiveness. *Marketing Science*, 30(3):413–415, 2011b.

Avi Goldfarb and Catherine E Tucker. Privacy regulation and online advertising. *Management science*, 57 (1):57–71, 2011c.

Marta C Gonzalez, Cesar A Hidalgo, and Albert-Laszlo Barabasi. Understanding individual human mobility patterns. *nature*, 453(7196):779, 2008.

Il-Horn Hann, Kai-Lung Hui, Sang-Yong T Lee, and Ivan PL Png. Consumer privacy and marketing avoidance: A static model. *Management Science*, 54(6):1094–1103, 2008.

Trevor Hastie, Saharon Rosset, Ji Zhu, and Hui Zou. Multi-class adaboost. *Statistics and its Interface*, 2(3): 349–360, 2009.

Donna L Hoffman, Thomas P Novak, and Marcos Peralta. Building consumer trust online. *Communications of the ACM*, 42(4):80–85, 1999.

Torsten Hothorn, Kurt Hornik, and Achim Zeileis. ctree: Conditional inference trees. *The Comprehensive R Archive Network*, pages 1–34, 2015.

Joakim Kalvenes and Amit Basu. Design of robust business-to-business electronic marketplaces with guaranteed privacy. *Management Science*, 52(11):1721–1736, 2006.

Kelsey. US Local Mobile Local Social Ad Forecast. `https://shop.biakelsey.com/product/2018-u-s-local-mobile-local-social-ad-forecast/`, 2018.

V Kumar, Xi Zhang, and Anita Luo. Modeling customer opt-in and opt-out in a permission-based marketing context. *Journal of Marketing Research*, 51(4):403–419, 2014.

Chen Li, Houtan Shirani-Mehr, and Xiaochun Yang. Protecting individual information against inference attacks in data publishing. In *International Conference on Database Systems for Advanced Applications*, pages 422–433. Springer, 2007.

Chenxi Li, Xueming Luo, Cheng Zhang, and Xiaoyi Wang. Sunny, rainy, and cloudy with a chance of mobile promotion effectiveness. *Marketing Science*, 36(5):762–779, 2017.

Tiancheng Li and Ninghui Li. Injector: Mining background knowledge for data anonymization. In *Data Engineering, 2008. ICDE 2008. IEEE 24th International Conference on*, pages 446–455. IEEE, 2008.

Tiancheng Li, Ninghui Li, Jian Zhang, and Ian Molloy. Slicing: A new approach for privacy preserving data publishing. *IEEE transactions on knowledge and data engineering*, 24(3):561–574, 2012.

Xiao-Bai Li and Sumit Sarkar. Privacy protection in data mining: A perturbation approach for categorical data. *Information Systems Research*, 17(3):254–270, 2006.

Xiao-Bai Li and Sumit Sarkar. Against classification attacks: A decision tree pruning approach to privacy protection in data mining. *Operations Research*, 57(6):1496–1509, 2009.

Xiao-Bai Li and Sumit Sarkar. Class-restricted clustering and microperturbation for data privacy. *Management science*, 59(4):796–812, 2013.

Andy Liaw, Matthew Wiener, et al. Classification and regression by randomforest. *R news*, 2(3):18–22, 2002.

Xueming Luo, Michelle Andrews, Zheng Fang, and Chee Wei Phang. Mobile targeting. *Management Science*, 60(7):1738–1756, 2014.

Ashwin Machanavajjhala, Johannes Gehrke, Daniel Kifer, and Muthuramakrishnan Venkitasubramaniam. ℓ-diversity: Privacy beyond κ-anonymity. In *null*, page 24. IEEE, 2006.

Ashwin Machanavajjhala, Johannes Gehrke, and Michaela Götz. Data publishing against realistic adversaries. *Proceedings of the VLDB Endowment*, 2(1):790–801, 2009.

Kelly D Martin, Abhishek Borah, and Robert W Palmatier. Data privacy: Effects on customer and firm performance. *Journal of Marketing*, 81(1):36–58, 2017.

Charles S Mayer and Charles H White Jr. The law of privacy and marketing research. *Journal of Marketing*, 33(2):1–4, 1969.

Syam Menon and Sumit Sarkar. Minimizing information loss and preserving privacy. *Management Science*, 53(1):101–116, 2007.

Amalia R Miller and Catherine Tucker. Privacy protection and technology diffusion: The case of electronic medical records. *Management Science*, 55(7):1077–1093, 2009.

Amalia R Miller and Catherine Tucker. Privacy protection, personalized medicine, and genetic testing. *Management Science*, 64(10):4648–4668, 2017.

Dominik Molitor, Philipp Reichhart, Martin Spann, and Anindya Ghose. Measuring the effectiveness of location-based advertising: A randomized field experiment. *Available at SSRN 2645281*, 2019.

Krishnamurty Muralidhar and Rathindra Sarathy. Data shufflinga new masking approach for numerical data. *Management Science*, 52(5):658–670, 2006.

Luca Pappalardo, Salvatore Rinzivillo, and Filippo Simini. Human mobility modelling: exploration and preferential return meet the gravity model. *Procedia Computer Science*, 83:934–939, 2016.

Roberto Pellungrini, Luca Pappalardo, Francesca Pratesi, and Anna Monreale. A data mining approach to assess privacy risk in human mobility data. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 9(3):31, 2018.

Pew. More Americans using smartphones for getting directions, streaming TV. `http://www.pewresearch.org/fact-tank/2016/01/29/us-smartphone-use/`, 2016.

Yi Qian and Hui Xie. Drive more effective data-based innovations: enhancing the utility of secure databases. *Management Science*, 61(3):520–541, 2015.

Omid Rafieian and Hema Yoganarasimhan. Targeting and privacy in mobile advertising. 2018.

General Data Protection Regulation Regulation. Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46. *Official Journal of the European Union (OJ)*, 59(1-88):294, 2016.

Pierangela Samarati. Protecting respondents identities in microdata release. *IEEE transactions on Knowledge and Data Engineering*, 13(6):1010–1027, 2001.

Pierangela Samarati and Latanya Sweeney. Generalizing data to provide anonymity when disclosing information. In *PODS*, volume 98, page 188. Citeseer, 1998.

Burhaneddin Sandıkçı, Lisa M Maillart, Andrew J Schaefer, and Mark S Roberts. Alleviating the patient's price of privacy through a partially observable waiting list. *Management Science*, 59(8):1836–1854, 2013.

Lalitha Sankar, S Raj Rajagopalan, and H Vincent Poor. Utility-privacy tradeoffs in databases: An information-theoretic approach. *IEEE Transactions on Information Forensics and Security*, 8(6):838–852, 2013.

Matthew J Schneider, Sharan Jagpal, Sachin Gupta, Shaobo Li, and Yan Yu. A flexible method for protecting marketing data: An application to point-of-sale data. *Marketing Science*, 37(1):153–171, 2018.

Miremad Soleymanian, Charles B Weinberg, and Ting Zhu. Sensor data and behavioral tracking: Does usage-based auto insurance benefit drivers? *Marketing Science*, 2019.

Statista. Share of smartphone users that use an Apple iPhone in the United States from 2014 to 2019. `https://www.statista.com/statistics/236550/percentage-of-us-population-that-own-a-iphone-smartphone/`, 2018.

Kyle Taylor and Laura Silver. Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally. `http://www.pewglobal.org/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/`, 2019.

Manolis Terrovitis, Nikos Mamoulis, and Panos Kalnis. Privacy-preserving anonymization of set-valued data. *Proceedings of the VLDB Endowment*, 1(1):115–125, 2008.

Manolis Terrovitis, Giorgos Poulis, Nikos Mamoulis, and Spiros Skiadopoulos. Local suppression and splitting techniques for privacy preserving publication of trajectories. *IEEE Trans. Knowl. Data Eng*, 29(7): 1466–1479, 2017.

Catherine E Tucker. Social networks, personalized advertising, and privacy controls. *Journal of Marketing Research*, 50(5):546–562, 2013.

Jennifer Valentino-Devries, Natasha Singer, Michael H. Keller, and Aaron Krolik. Your Apps Know Where You Were Last Night, and Theyre Not Keeping It Secret. `https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html?smid=re-nytimes`, 2018.

Verge. Android Q leak reveals system-wide dark mode and bigger emphasis on privacy . `https://www.theverge.com/2019/1/16/18185763/android-q-leak-dark-mode-new-privacy-settings`, 2019.

Dashun Wang, Dino Pedreschi, Chaoming Song, Fosca Giannotti, and Albert-Laszlo Barabasi. Human mobility, social ties, and link prediction. In *Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 1100–1108. Acm, 2011.

Ke Wang, Benjamin CM Fung, and S Yu Philip. Handicapping attacker's confidence: an alternative to k-anonymization. *Knowledge and Information Systems*, 11(3):345–368, 2007.

Mingzheng Wang, Zhengrui Jiang, Yu Zhang, and Haifang Yang. T-closeness slicing: A new privacy-preserving approach for transactional data publishing. *INFORMS Journal on Computing*, 30(3):438–453, 2018.

Michel Wedel and PK Kannan. Marketing analytics for data-rich environments. *Journal of Marketing*, 80 (6):97–121, 2016.

Nathalie E Williams, Timothy A Thomas, Matthew Dunbar, Nathan Eagle, and Adrian Dobra. Measures of human mobility using mobile phone records enhanced with gis data. *PloS one*, 10(7):e0133630, 2015.

David Jingjun Xu. The influence of personalization in affecting consumer attitudes toward mobile advertising in china. *Journal of Computer Information Systems*, 47(2):9–19, 2006.

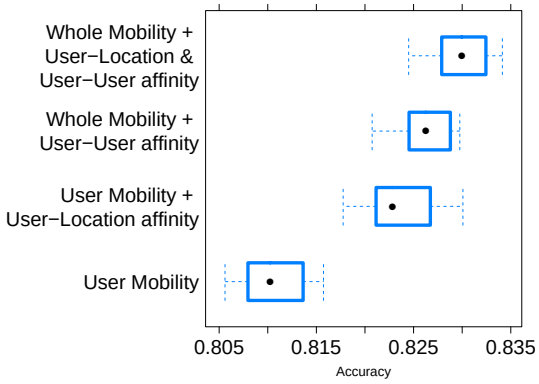
Dingqi Yang, Bingqing Qu, and Philippe Cudre-Mauroux. Privacy-preserving social media data publishing for personalized ranking-based recommendation. *IEEE Transactions on Knowledge and Data Engineering*, 2018.

Roman Yarovoy, Francesco Bonchi, Laks VS Lakshmanan, and Wendy Hui Wang. Anonymizing moving objects: How to hide a mob in a crowd? In *Proceedings of the 12th International Conference on Extending Database Technology: Advances in Database Technology*, pages 72–83. ACM, 2009.

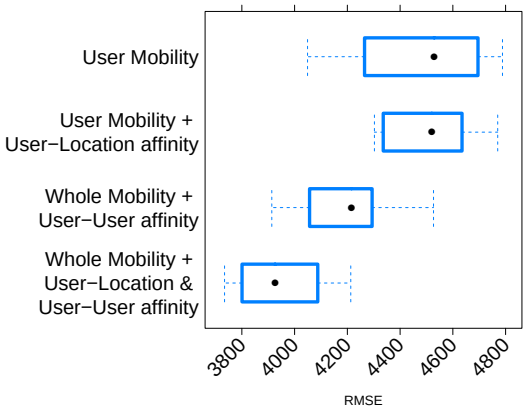
Yu Zheng, Xing Xie, and Wei-Ying Ma. Geolife: A collaborative social networking service among user, location and trajectory. *IEEE Data Eng. Bull.*, 33(2):32–39, 2010.

Appendix A: Model choices in proposed framework

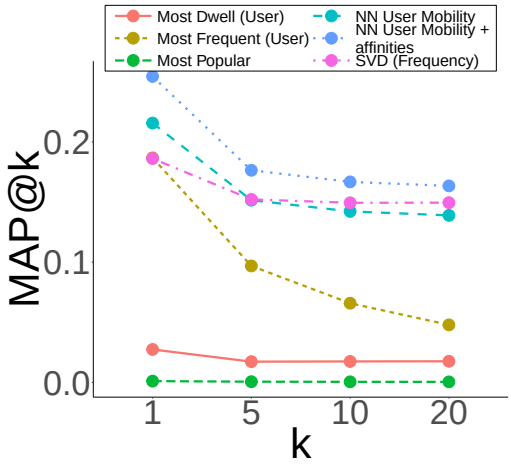
We empirically justify the model choices made in our methodology. All the choices were made based by assessing the performance of different machine learning heuristics used in our framework on non-obfuscated data. First, in Figures 6a, 6b we show the incremental benefit of the affinity features discussed in the feature extraction $\mathcal{F}(T)$. Figure 6a shows the accuracy of the Random Forest classifier to predict the operating system of a user. The model was regularized by performing a grid search on the maximum number of features and trees [24] via five-fold cross-validation. The best performing model has an accuracy of 82% which indicates the success a privacy attacker would have in inferring the unpublished operating system of a user from trajectory data. In Figure 6b, we plot the RMSE of the Random Forest regressor trained to predict the home address of a user.[25]



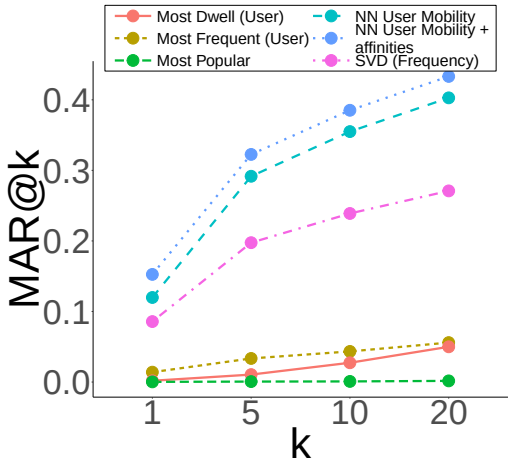
(a) OS inference threat - Model Accuracy



(b) Home address inference - Model RMSE



(c) $MAP@k$ POI Recommendation model



(d) $MAR@k$ POI Recommendation model

Figure 6 Proposed framework model choices

[24] Grid for fraction of features - $\{.25, .5, .75, 1\}$, trees - $\{50, 100, 200\}$

[25] We infer the ground truth of home location in our data by assigning this to be the most frequently visited location during 10 PM - 6 AM for each user. We have already tested alternative time periods such as 11 PM - 5 AM, and the results remain robust. We also delete the inferred home location from all user trajectories for our experiments.

Next, we learn two regression models to predict the Universal Transverse Mercator (UTM) transformed latitude and longitude of the home location with similar hyperparameter tuning as earlier. The error estimate is the Euclidean distance between the estimated and assigned home UTM coordinates. From the box plots of the re-sampled performance measures (Figures 6a, 6b), we notice that the User-User and User-Location affinity features incrementally improve the performance of both the proxy models learned. In Figures 6c, 6d, we visualize the $MAP@k$ and $MAR@k$ of the neighborhood-based recommendation model learned by tuning the number of neighbors.

We compare the performance with several baselines - recommendations based on the most popular locations (Most Popular), based on the locations that the user spent the most time in (Most Dwell (User)), visited most frequently (Most Frequent (User)) and an SVD on the user-location matrix populated with frequency. We observe that the NN based model performs better in both the metrics compared to the baselines justifying the choice. The RMSE, 3,900 meters $\approx$ 2.46 miles indicates the success an attacker would have in identifying the home location of a user from non-obufuscated data. Further, we also notice the incremental benefit (See NN User Mobility vs NN User Mobility + affinities in Figures 6c, 6d) of the affinity features in the recommendation performance.

Appendix B: Utility measurement

We compute the data utility under different obfuscations. We estimate this by computing the performance of a neighborhood-based collaborative filtering recommendation heuristic to accurately predict future user locations. To assess the accuracy of predictions made, we treat the locations visited by each user in the fifth week as ground truth and train the recommender model to predict these locations.

Based on the user risks, we obfuscate T_{train} by varying $p \in \mathcal{G}_p$. We learn a neighborhood-based recommender (Bobadilla et al. 2011) tuning number of neighbors by five-fold cross-validation on the obfuscated training sample $\mathcal{P}(T_{train})$. The model is learned to rank locations a user is likely to visit in the fifth week of the observation period. That is, we build features, $\mathcal{F}(P(T_{train}))$ on first four weeks and tune number of neighbors[26] to maximize prediction accuracy. Then, we compute utility —$MAP@k$, $MAR@k$ on T_{test} for $k = \{1, 5, 10\}$[27]. Intuitively, $MAP@1$ and $MAR@1$, for example, represent advertiser's utility to predict next location a user is most likely to visit in the fifth week based of the recommender model that was learned on the obfuscated data. A key detail in the utility estimation is that we do not perform any obfuscation on T_{test} for any value of p since our aim is to quantify the ability of obfuscated data, $\mathcal{P}(T_{train})$ to learn true preferences of a user, which are revealed in the non-obfuscated test sample. Similar to risk, we perform twenty trials for each p and report mean and 95% confidence intervals of utility metrics in Figure 3.

[26] Grid for number of neighbors - $\{5, 10, 25, 50, 100, 200\}$

[27] The learned recommender model can be used to compute $MAP@k$, $MAR@k$ for other values of k as well. We consider $k = \{1, 5, 10\}$ for illustration of the method's efficacy.