TechXplore

Amid volumes of mobile location data, new framework reduces consumers' privacy risk, preserves advertisers' utility

June 5 2023

Credit: CC0 Public Domain

The use of mobile technologies to collect and analyze individuals' location information has produced massive amounts of consumer location data, giving rise to an elaborate multi-billion-dollar system in which consumers can share personal data in exchange for economic benefits. But privacy risks prevail.

In a new study, researchers have used machine learning to create and test a framework that quantifies personalized privacy risks; performs personalized data obfuscation; and accommodates a variety of risks, utilities, and acceptable levels of risk-utility tradeoff. The framework outperformed prior models, significantly reducing consumers' privacy risk while preserving advertisers' utility.

The study was conducted by researchers at Carnegie Mellon University (CMU), the University of Virginia, and New York University. It is published in *Information Systems Research*.

"The global market for location analytics alone is projected to reach $25.5 billion by 2027," notes Beibei Li, associate professor of IT and management at CMU's Heinz College, who co-authored the study. "As industries increasingly unleash the power of location big data, our study offers a much-needed framework to balance privacy risks and data utilities, and to sustain a secure and self-governing multi-billion-dollar location ecosystem."

Massive volumes of mobile location data are being generated daily through smartphone location-based services (e.g., navigation, ride share, food delivery services). Such data track consumers' behavior—where they eat and shop, what products they buy—to enable applications of commercial value (e.g., restaurant recommendations, location-based advertising, market research). Advertisers who gain access to location data through data aggregators can predict consumers' next location with 25% success and next activity and timing with 26% success.

But there are considerable risks to consumers of sharing location data, which includes personally identifiable information like names and home addresses. Some advertisers may carry out malicious acts using the data, usually for short-term revenue gains. Therefore, data aggregators need a personalized and flexible framework to balance diverse types of risks and utilities for different kinds of consumers and advertisers.

In this study, researchers developed a machine learning-based framework that quantifies individual consumers' privacy risk, quantifies advertisers' utility, and features a personalized and flexible obfuscation scheme. The scheme suppresses a subset of locations visited by a consumer based on his or her personalized suppression parameter proportional to the individual's risk level; it also accommodates different types and different acceptable levels of risks and utilities.

To test their framework, researchers partnered with a leading data aggregator that integrates location data across more than 400 commonly used mobile apps (e.g., news, weather, maps, fitness) from a quarter of the U.S. population who are in compliance with privacy regulations. The data, collected in five weeks from September to October 2018, are representative of the U.S. population and the sample analyzed covers a major U.S. metropolitan area. Researchers validated the framework on a million trajectories (where and when consumers move) generated by 40,000 consumers in a major U.S. metropolitan area.

The study's framework accounts for distinct characteristics of individual-level location data, and outperforms multiple benchmark methods from recent studies, according to the authors.

Using the proposed framework, the authors say, a data aggregator can effectively curtail a potential invasion of consumer privacy by performing personalized data obfuscation without sacrificing the utility of the obfuscated data to an advertiser. The aggregator may also fulfill personalized and diverse demands from both consumers and advertisers by flexibly accommodating multiple types of risks and utilities, as well as a wide array of acceptable levels of a specific risk, utility, and risk-utility tradeoff.

"Location-based marketing is rapidly becoming a primary venue for planning marketing campaigns and targeting consumers, enriching both traditional and digital marketing strategies," explains Meghanath Macha, a graduate of CMU's Heinz College, who led the study. "Our framework fills a critical void and offers an important tool for the privacy-aware practices of big data location-based applications and services, providing a balance between privacy risks and data utilities."

Among the study's limitations, the authors note that the data they used contain no information about individual consumers' demographics, which would allow greater understanding of privacy issues. In addition, their proposed framework considered only one-shot data sharing with an advertiser; it did not consider more complex scenarios with multiple risks or utilities, or what happens when an advertiser combines multiple batches or sources of shared data.

More information: Meghanath Macha et al, Personalized Privacy Preservation in Consumer Mobile Trajectories, *Information Systems Research* (2023). DOI: 10.1287/isre.2023.1227

Provided by Carnegie Mellon University's Heinz College

Citation: Amid volumes of mobile location data, new framework reduces consumers' privacy risk, preserves advertisers' utility (2023, June 5) retrieved 20 March 2024 from https://techxplore.com/news/2023-06-volumes-mobile-framework-consumers-privacy.html