# Introduction to the Special Issue on Privacy and Security for Location-based Services and Devices

The evolution of mobile phones into smartphones, and the diffusion of location-based services (LBS), are cornerstones of the digital era, but at the same time introduced a number of challenges to the privacy of individuals. Traditional information (as names, addresses and phone numbers) shared across the Internet with an increased number of services is now frequently coupled with positional data.

With such detailed information, service providers are able to infer with alarming precision a number of sensitive information about their users, including religious, sexual and political preferences, as well as details of their social relationships and private life in general.

To the extreme, this can lead to manipulation and threats to an individual's autonomy and freedom. When certain privileged actors with access to this information can learn everything about us, their actions can directly condition our everyday life, making factitious and unnatural. Privacy-preserving and secure location-based services are thus essential in allowing us to enjoy the many benefits of the digital era, while preventing threats to our fundamental rights.

A number of articles were selected for this Special Issue, each of which makes a significant contribution to the debate on new directions in location privacy. Some articles are significantly extended versions of papers presented at the 2019 Location Privacy Workshop (LPW), while others are original contributions.

Specifically, we received 15 original research papers that underwent two rounds of reviews, performed by 40 independent experts within the field. Among the received submissions, 8 papers were selected for publication in the Special Issue, resulting in an acceptance rate of approximately 50%.

Through and in-depth analysis of involved regulations and patents, S. Wicker investigates the impact of location information disclosure with respect to e-book readers and shows how this tracking may infringe freedom of association. The study is specifically devoted to the study of Amazon Kindle device and discusses privacy implications within the US and European law domain.

X. Xiong et al. propose a novel of definition of $(\epsilon, \delta)$-local differential privacy with the ability to capture the temporal correlation in spatio-temporal data. The authors also develop an efficient framework for real-time and private spatio-temporal data aggregation with an untrusted server. The study is accompanied by several experiments on two real-world datasets to evaluate the framework.

The studies proposed by M. Babaghayou et al. and by L. Sleem et al. are instead devoted to Vehicular Ad-hoc Networks, a promising field of application within the Intelligent Transportation Systems domain. As several privacy issues remain to be solved before VANET becomes fully applicable, the authors propose two surveys on the subject. Specifically, M. Babaghayou et al. propose a novel taxonomy to classify the privacy-preserving strategies within this field while L. Sleem et al. focus on several solutions that may be applied to various attacks concerning Internet of Vehicles.

M. Caesar and J. Steffan investigate privacy implications of smartphones applications relying on the Bluetooth technology for indoor positioning. As Bluetooth Low Energy beacons enable very accurate indoor positioning, the authors argue a Bluetooth Mesh network could inadvertently serve the same purpose, leading to unexpected location privacy violations. This assumption is proved analyzing the information broadcasted by a typical Bluetooth Mesh through a malicious smartphone app that is able to localize a smartphone user within a building. The paper also includes a randomization strategy solve this issue.

L. Calderoni et al. discuss data processing techniques relying on probabilistic data structures designed to mitigate the user's privacy leakage in indoor localization. The amount of privacy is mea-

sured through two privacy metrics: size of uncertainty region and $\gamma$-deniability. The proposed system is also discussed according to the privacy-by-design and privacy-by-default paradigms, in relation to privacy regulations such as the GDPR. The supporting experiments were carried out in a real-world environment using off-the-shelf networking equipment, in combination with several primitives designed to passively infer and collect the user position.

Boutet and Cunche propose a novel solution to preserve users' privacy in Wi-Fi-based positioning systems. Their technique combines a caching strategy (for limiting the exposure of the users position for already visited locations) and random sampling (for controlling the precision of revealed information). The proposed approach can reduce significantly the exposure of the user's location to positioning systems (up to 95%).

Gallinucci et al. present an attack against anonymized location information, reminding us of the importance of strong privacy guarantees to be adopted when releasing such data. In particular, they propose an innovative approach to de-anonymize personal gazetteers (the set of main points of interest) of users of social media through their social trajectories, even in absence of a temporal alignment between the two sources (i.e., they have been collected over different time periods).

To conclude, the papers included in this special issue contribute by highlighting the challenges of preserving privacy in location-based services and applications from a number of different perspectives. They provide readers with an overview of the complex challenges and possible solutions in the exciting and evolving domain of location privacy.

The Guest Editors:

Luca Calderoni
*University of Bologna, Italy*

Paolo Palmieri
*University College Cork, Ireland*

Constantinos Patsakis
*University of Piraeus, Greece*