ISSN 2704-8012

European Journal of Privacy Law & Technologies

2019/2



G. Giappichelli Editore

European Journal of Privacy Law & Technologies

Directed by Lucilla Gatt

2019/2

G. Giappichelli Editore

European Journal of Privacy Law & Technologies
On line journal
Italian R.O.C. n. 25223

G. GIAPPICHELLI EDITORE - TORINO
VIA PO, 21 - TEL. 011-81.53.111 - FAX 011-81.25.100
http://www.giappichelli.it



The Journal is one of the results of the European project TAtoDPR (Training Activities to Implement the Data Protection Reform) that has received funding from the European Union's within the REC (Rights, Equality and Citizenship) Programme, under Grant Agreement No. 769191.

The contents of this Journal represent the views of the author only and are his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

Published Online by G. Giappichelli in Dicember 2019
www.ejplt.tatodpr.eu

LOCATION DATA PRIVACY ON MAAS UNDER GDPR

Erion Murati e Manjola Hënkoja

Abstract

Mobility as a Service (MaaS) is a new transport paradigm that integrates existing and new mobility services into one single digital platform, providing customised door-to-door transport and offering personalised trip planning and payment options. The development of MaaS relies heavily on access to user's data, open APIs of transport providers and interoperability of the systems. Since data are the key factor of MaaS, establishing clear and fair rules for the control of information is crucial. MaaS is a location-based service (LBS) navigation which uses real-time geo-data from a mobile device to provide user's location and other information. Under Article 4 of the GDPR, location data is expressly mentioned as a factor by reference to which a person may be directly or indirectly identified, thus is recognised as an 'identifier' of personal data. The aim of this chapter is to overview and analyse the privacy vulnerabilities of location data which may become sensitive data on MaaS in combination with other information. Further, this paper will analyse the guarantees provided by GDPR, either strictly legal (i.e. consent of the data subject) or technological (i.e. DPIA) and their reliability to protect user's identity.

Key-words: Navigation apps, Location Based Services, Data Location, MaaS, DPIA.

Summary: 1. Introduction. – 2. The key role of data on MaaS. – 3. Collecting and using personal location-based data. – 4. Privacy and data protection risks. – 5. Personal location data under GDPR. – 5.1. Sensitive location data. – 5.2 Legal justifications for location data processing. – 5.3. DPIA. – 5.4. Anonymization and Pseudonymization Location Privacy. – 6. Conclusion.

1. Introduction

An old saying says that the key to making it through life is to know where you are, where you've been, and where you're going. In today's digital world, there is an app for that. Advances in ICTs have enabled significant developments in geo-localization systems, which are increasingly embedded in smartphones and have paved the way for the development of new transport op-

tions [1] relying on the sharing of a specific asset (which can be a vehicle) or of a dedicated service (i.e. a ride), that is to say new consumption patterns. Recent research confirms an emerging picture of a possible correlation between the growth momentum of new mobility service providers and their relative dependence on mobile ICT, whereby those companies with the greatest dependence on smartphones and mobile apps are those attracting the most funds and developing the fastest. [2] Shared mobility clearly stress access over ownership and highlight the role of ICT in its development. More people are starting their trips with smartphones [3] to plan routes, seek departure information for the next bus or railcar, find a taxi via an e-Hail app, or source a private driver through services, such as Uber. Factors driving transportation app growth include: time savings (e.g., high occupancy vehicle lanes available to users of dynamic ridesharing); financial savings (e.g., dynamic pricing providing discounts for peak and off-peak travel and for choosing low-volume routes); incentives (e.g., offering points, discounts, or lotteries). For public agencies, transportation apps can aid network management functions, such as disseminating roadway and public transportation information on incidents, delays, congestion, and service disruptions. [4] For mobility users, the purpose of these apps is to facilitate door-to-door mobility by giving people greater control over their trips, through "real-time" access information and coordination, previously unavailable [5] (such as estimated departure and arrival times, comparison of routes and modal options.). Moreover, scientific research studies suggest that ICT technology is influencing traveller's behaviour when it comes to transportation choices. Reliable and tailored information, offered by ICT, allow users to make active decisions, thereby exercising a form of control on their personal outcomes. [6] This emerging mobility

[1] M. Finger, M. Audouin, *The Governance of Smart Transportation Systems Towards New Organizational Structures for the Development of Shared, Automated, Electric and Integrated Mobility* (Springer 2019) 2.

[2] V. Boutile, 'New Mobility Services', in A Aguilera, V Boutile, *Urban Mobility and the Smartphone*, (Elsevier 2018), 40-45.

[3] H. Pfriemer, 'The Digital Economy and the Promise of a New Mobility' in B Flügge (ed.), *Smart Mobility – Connecting Everyone* (Springer 2017) 73.

[4] S. Shaheen, S. Cohen, A. Martin, 'Smartphone app evolution and early understanding from a multimodal app user survey', in G Meyer and S Shaheen, *Disrupting Mobility* (Springer 2017) 150.

[5] A. Aguilera, 'Smartphone and Individual Travel Behaviour', in A. Aguilera, V. Boutile, *Urban Mobility and the Smartphone* (Elsevier 2018) 7-8.

[6] A.L. Davidson, (2017) 'Getting Around with Maps and Apps: How ICT Sways Mode Choice' in G Meyer, S Shaheen, *Disrupting Mobility* (Springer 2017) 178; See also, D Ettema, *Apps, activities and travel: an conceptual exploration based on activity theory* (Springer Transportation 2018) V 45, 273-290.

ecosystem can deliver many benefits for traditional transport service providers as well, including integrated payment scheme, developing better first-mile/last-mile and enhancing the richness of transportation data. [7]

Mobility as a Service (MaaS) concept has risen from the recent mobility tendency, promising an integrated flexible mobility platform. [8] The complexity of using a variety of transport modes, different payment methods and lack of integrated information discourages many people from using them. The key is to integrate the various transport modes in a way that creates seamless door to door journey experiences for users through a MaaS platform. Basically, integrated mobility aims to enable multimodal travel [9] – defined as the use of more than one travel mode for passenger or goods movement – and produce a shift from private motorized travel to more sustainable modes of travel such as public transport or shared mobility modes. According to Finger [10] (2019) integrated mobility has basically been facilitated recently by two main ICT-supported developments: the development of integrated multimodal information systems, and integrated payment solutions. While the former has enabled users to access and compare specific travel information in real time from different transport providers, and therefore pick the solution best fitting their mobility needs [11] the latter has enabled users to access various transportation solutions with a single ticketing means, which could be a card (smart card) or a dedicated app. Put together, and also supported by the birth of new shared mobility solutions, those two ICT-supported developments have enabled the unfolding of the Mobility-as-a-Service (MaaS) concept. Shared mobility, automated mobility, electric mobility and integrated transport are the four pillars which will contribute to shape the concept of smart mobility: zero emissions, zero accidents and zero ownership. [12] According to the House of Commons report [13] (2018) on MaaS in-

---

[7] M. Dinning, T. Weisenberger, 'Multimodal Transportation Payments Convergence-Key to Mobility' in G. Meyer and S. Shaheen, *Disrupting Mobility* (Springer 2017) 120-122.

[8] S.H. Fariya, M. Henk, 'The Governance of Demand-Responsive Transit Systems-A Multi-level perspective' in M. Finger & M. Audoin, *The Governance of Smart Transportation Systems* (Springer 2019) 1.

[9] S. Shaheen, and others, *Mobile Apps and Transportation: A Review of Smartphone Apps and A Study of User Response to Multimodal Traveler Information*, (California 2016) 13.

[10] M. Finger, M. Audouin, *The Governance of Smart Transportation Systems Towards New Organizational Structures for the Development of Shared, Automated, Electric and Integrated Mobility* (Springer 2019) 3.

[11] S. Kenyon, G Lyons, *The value of integrated multimodal traveller information and its potential contribution to modal change* (Transp. Res. 2003) 1-21.

[12] L. Neckermann, The mobility revolution zero emissions, zero accidents, zero ownership in https://www.troubador.co.uk/bookshop/computing-science-education/the-mobility-revolution/Accessed August 2019.

quiry the MaaS ecosystem is made up of: 1) customers; 2) MaaS platform providers: who design and offer the MaaS platform (app or website) and create packages based on customer demands; 3) data providers: who share and use data, which is crucial to MaaS, 4) and a range of transport operators; The combination of these new technologies allows a mobility which is in no way inferior to the freedom promised by the private car. To meet a customer's request, a MaaS operator facilitates a diverse menu of transport options, be they public transport, ride –, car – or bike-sharing, taxi, car rental or lease, or a combination thereof, accessible *on demand*. Since MaaS concept is holistic and still emerging, it can be defined and approached from many different points of view, however the definition used in this chapter is the same definition adopted in MaaSiFiE project, namely: "Multimodal and sustainable mobility services addressing customers' transport needs by integrating planning and payment on a one-stop-shop principle" [14] Since 2014 when MaaS concept was officially introduced to the public at the 2014 ITS European congress in Helsinki [15] MaaS has received much attention within and around the transportation industry. Proponents argue that MaaS will become the new transport paradigm since it addresses many of society's grand challenges in transport, promising improvements in terms of environmental sustainability, reduced congestion and better accessibility. [16] It has also been argued that the diffusion of MaaS may completely change both how we travel and how personal transportation is organized and that MaaS could be an emerging trillion-dollar industry at the expense of the incumbent private car sector. [17] However, alongside the benefits comes also the drawbacks. The main objective of this chapter is to analyse the privacy vulnerabilities of location data

[13] Mobility as a Service inquiry in https://www.parliament.uk/business/committees/committees-a-z/commons-select/transport-committee/inquiries/parliament-2017/mobility-as-a-service-17-19/Accessible December 2018.

[14] D König and others, *Deliverable 3: Business and operator models for MaaS* (MAASiFiE 2016) 1-10.

[15] M Audouin, *Towards Mobility-as-a-Service: a cross-case analysis of public authorities' roles in the development of ICT-supported integrated mobility schemes* (2019) in https://infoscience.epfl.ch/record/264957 Accessed August 2019 163.

[16] Polis, *Mobility as a service: Implications for urban and regional transport. Brussels* in Polis network 2017 Retrieved from https://www.polisnetwork.eu/uploads/Modules/PublicDocuments/polis-maas-discussion-paper-2017---final_.pdf Accessed September 2019; See also, MaaS Alliance (2017 September 4) *White Paper: Guidelines & Recommendations to create the foundations for a thriving MaaS Ecosystem* in *MaaS Alliance* 2017, Retrieved from https://maas-alliance.eu/wp-content/uploads/sites/7/2017/09/MaaS-WhitePaper_final_040917-2.pdf Accessed August 2019.

[17] G Smith and others, 'Governing Mobility-as-a-Service: Insights from Sweden and Finland' in M Finger M Audouin (eds) *The Governance of Smart Transportation Systems* (Springer 2019) 170.

and to shed lights on the impact that GDPR is having on MaaS provider which may use location data to monitor user's travel behaviour or to identify and process sensitive data patterns. In the next section the key role of data on MaaS is discussed. In section 3 the way location data is collected and used, under section 4 potential privacy risks arising to location data via LSB. Furthermore, an analyse of GDPR has been conducted in regard to the protection of personal location and/or sensitive data, with its legal remedies and technical guarantees.

2. The key role of data on MaaS

Data means (electronically) stored information, signs or indications. For MaaS to be successful a wide range of transport data is required. [18] The MaaS app basically enables customers to access information about what mobility solutions are available for the trip they are planning to make, thanks to an embedded routing system, as well as directly book the solution of their choice, and pay for it, all in the same app. From a technological perspective, MaaS providers position themselves on two different fronts. On one hand, MaaS providers basically integrate data, such as routes, real time user'/vehicle's position, speed, transfer time and as well as the application programming interfaces (APIs) of the different transport operators, both previously made open by them. APIs represent a set of processes that govern the interactions between different web-based services [19] and put together constitute what is referred to as the back-end, also sometimes called the data platform or data layer, that MaaS providers operate. Therefore, sharing of APIs allows MaaS providers to offer customers a single digital interface for planning, booking, paying for and using transport. [20] On the other hand, MaaS providers also take care of building the app and the website that comes on top of the back-end, which is the major customer interface, referred to as front-end.

The most important policy designed at the national level to enable the development of MaaS, via deregulation, is the new Finnish Transport Act, entered into force in 2018. [21] The Code focuses on enhancing the use of open data and oblige mobility operators to provide their operational data as well as their single tickets for third-party resale and use. The main idea of the Code is to take ad-

[18] M. Kamargianni, M. Matyas, *The potential of mobility as a service bundles as a mobility management tool* (Springer 2018) 1-16.

[19] D. König and others, *Deliverable 5: Technology for MaaS* (MAASiFiE 2016) 21.

[20] M. Kamargianni, *The potential of mobility as a service bundles as a mobility management tool* (n. 18) 2.

[21] LVM 2017a Finnish Transport Code. Act on Transport Services https://www.lvm.fi/lvm-site62-mahti-portlet/download?did=246709 Accessed August 2019.

vantage of digitalization and enable both the development of better and more agile transport services, and the integration of them into MaaS offerings, with the concrete goals of achieving a 10% savings in publicly subsidized passenger transport from 2017.[22] The finish transport code (2017), can be understood as a real push towards MaaS, for three main reasons. Firstly, it enables the size of the for-hire vehicles fleet to grow as any type of vehicle is allowed to be used as a taxi by removing the existing quota that has been limiting their total number of licenses in Finland (Chapter 1, Section 1). For-hire services are an important part of MaaS as they might bring a solution to the last-mile problem. Secondly, the text is seen as MaaS enabler as it forces all transport services providers to open essential data such as routes, timetables, stops, and fares in a computer-readable format (Chapter 2, section 1). Thirdly, it lays down provisions for the interoperability of ticketing systems, by requiring all public transport providers to open their single tickets APIs (Section 2). In 2018 the second part of the Code was approved (amendment n. 301/2018) and in *Section 2 a* was introduced the concept of acting in someone else's behalf, forcing transport providers to open up also seasonal tickets APIs. In a nutshell, MaaS concept lies on the idea of open data in transport industry. According to the European data portal definition[23], open data can be defined as "data that be freely used, modified, and shared by anyone for any purpose subject, at most, to measures that preserve provenance and openness". In other words, open data is data that can be accessed, shared, used and reused without any barrier for any type of (re)user. However, in a digital economy, the ownership and access to data determines the market dominance. Therefore, referring to MaaS Alliance[24] view it should be understood that data sharing does not necessarily equal to free data, but data sharing and exchange models should be designed between partners to be fair and to fit for purpose. The Code has predicted these concerns and according to Section 4, access to information and information systems offered through the open interfaces shall be offered on fair, reasonable and non-discriminatory terms. Alongside the need for data sharing and openness comes the need for data security, especially when it comes to user data. The International Transport Forum[25] (2016) outlines a number of factors which contribute to transport data

[22] G Smith and others, *Mobility as a service: Comparing developments in Sweden and Finland* (RTMB 2018) 40.

[23] European Data Portal, 2018, Open data in a nutshell https://www.europeandataportal.eu/en/providing-data/goldbook/open-data-nutshell Accessed August 2019.

[24] MaaS Alliance (2018, November) Data Makes MaaS happen, *in MaaS Alliance* https://maas-alliance.eu/wp-content/uploads/sites/7/2018/11/Data-MaaS-FINAL-after-plenary-1.pdf Accessed August 2019 Accessed August 2019.

[25] International Transport Forum, *Data Driven Transport Policy* Available at: https://www.itf

security: 1) Data minimization, collecting the minimum amount of data required and dispose it when it is no longer relevant; 2) De-identification/Anonymization, removing personal details associated with data, achieved through aggregation; 3) Encryption, encoding information so that only authorised parties can access it; 4) Transparency in "terms of use", making it clearer to people what data they are consenting to being shared.

3. Collecting and using personal location-based data

Location history is one of the prime bits of data any business can get on you, whether they want to personalize your weather reports, serve up an ad for a local restaurant or direction to parks. These services are known as location-based services (LBS) which are based on the user's current position to provide location-aware information. [26] As a result, apps and mobile Operator Systems (OS) are very keen to get hold of it. It's a compromise though, and if you don't want to give it away, you'll have to do without some location-based services (like directions to the parks, restaurants, museums and cities). The choice to be made is between convenience or privacy? You can't have both, but it is important to understand who can access this information, and what steps can be taken to ensure that only authorized parties can access it. The rise of LBSs is evident as 90 % of smartphone users polled said they used their device to find LBSs, such directions or local recommendations. [27] A recent survey by The Manifest [28] confirms that LBS navigation has become a staple for more than three-quarters of mobile users, with Google Maps being the overwhelming choice for mobile users. On MaaS ecosystem referring to scientific papers [29] real time user' and vehicle's position, allows MaaS provider to determine how far away vehicles are from customers

oecd.org/sites/default/files/docs/data-driven-transport-policy.pdf Accessed 24 August 2019. Accessed August 2019 23-26.

[26] C Bettini, S Mascetti, X Wang, 'Privacy Threats in Location-Based Services' in S. Shekhar, H. Xiong, (eds) *Encyclopedia of GIS* (Springer 2008).

[27] Marketer report (2016) Most smartphone owners use LBSs, https://www.emarketer.com/Article/Most-Smartphone-Owners-Use-Location-Based-Services/1013863 Accessed August 2019.

[28] P Riley, The popularity of Google Maps: trends in navigation Apps in 2018 (2018, July 10) https://themanifest.com/app-development/popularity-google-maps-trends-navigation-apps-2018Accessed August 2019.

[29] Transport Systems Catapult (2016). Mobility as a Service: Exploring the opportunity for Mobility as a Service in the UK [Online] Available at: https://ts.catapult.org.uk/wpcontent/uploads/2016/07/Mobility-as-a-Service_Exploring-the-Opportunity-for-MaaS-in-the-UK- Web.pdf Accessed August 2019; See also, M. Kamargianni, M. Matyas, *The potential of mobility as a service bundles as a mobility management tool* (Springer 2018) 1-16.

and thus estimate what time they will arrive (when combined with speed data). Moreover, thanks to location data MaaS provider could capture users' historical travel behaviour to better predict future travel patterns, modelling travel behaviour to forecast how users travel in time and space, understanding also the factors that influence on travel-related choices. For instance, the MaaS provider could incentive its user to use sustainable means of transportation – i.e. bike sharing –, giving some transport credit points for each km ridden. In performing that task, MaaS provider needs to know how many km a user is riding for a certain time. GPS, Bluetooth (used the latter, for example, by Mobike app for the ride of its free flow bikes) and other dynamic data will assist MaaS provider in order to fulfil this goal. This practice takes place in Bologna, in Italy, which rewards bike runners with free beers in exchange of the credit points accumulated during the ride. [30] Finally, geodata suggest users' most convenient route to be taken or to reroute her/him in case of a transport disruption to the final destination.

Generally, the term 'location data' comprises any information implicitly or explicitly referring to geographic or geospatial position. More specifically, according to Location Forum [31] location data is any data with an implicit or explicit geographic or geospatial reference, including any data derived from GPS, GIS, cell-tower or other radio signal based triangulation, assisted GPS positioning devices, systems and processes, geo-tagged images, video, audio and text documents, satellite and aerial imagery, computerized, digitized and paper maps, IP address location, public documents, public or private databases, video, audio, text and image files, location-based applications. However, personal location data is any information about a natural person's current or past geographical location or movements. [32] Technically, the monitoring can be done secretively, without informing the owner. Monitoring can also be done semi-secretively, when people "forget" or are not properly informed that location services are switched "on", or when the accessibility settings of location data are changed from "private' to 'public". For instance, according to a recent investigation of the Guardian [33], Facebook targets users with LBSs adverts even if they block the

[30] M. Buck A Bologna birra gratis per chi si muove in bicicletta (2018 December 7) https://www.welovecycling.com/it/ciclismo-urbano/2018/12/07/a-bologna-birra-gratis-per-chi-si-muove-in-bicicletta/ Accessed August 2019.

[31] Location Forum, *Location Data Privacy Guidelines, Assessments and Recommendations* (Version 2, 1 May 2013) 7.

[32] E. Morriessey, (2016) *Data protection issues Guidance on Location Data*, in https://www.fieldfisher.ie/data-protection-office-issues-guidance-location-data/ Accessed September 2019.

[33] The Guardian, (2019) Facebook users cannot avoid location-based ads, investigation finds, https://www.theguardian.com/technology/2018/dec/19/facebook-users-avoid-location-based-adssettings-investigation-reveals Accessed September 2019.

company from accessing GPS on their phones, turn off location history in the app, hide their work location on their profile and never use the company's "check in" feature. There is no combination of settings that users can enable to prevent their location data from being used by advertisers to target them. According to Chrétien [34], within the smartphone world geolocating applications fall into two categories depending on their purpose: either "statistical" in the sense of data collected by public authorities and designed for public policy or "business." Within the "business" category, there are four kinds of purposes: 1) mobility assistants, from map location to path identification (Google Maps, Apple Plans) and en-route guidance; 2) location-based services (LBS), advising the user on the best or closest service (e.g., restaurants, shopping or touristic activities); 3) self-monitoring of activities, such as running; 4) marketing analysis of user's activities and spatial practices, so as to detect his or her consumption styles, tastes, and desires. Differently, other scholars [35] put together all geolocating applications within the concept of LBSs. However, if referred to Chrétien's classification – technically more precise-, MaaS providers could also add in their platform LBSs and marketing analysis of user's activities and spatial practices. Location information may represent some of the most sensitive data collected and stored by transportation apps and shared with third parties to offer users additional products and services. Privacy and security concerns are complicated by this type of data sharing because this is often facilitated through third-party APIs, which may contain security vulnerabilities in addition to the cloud, software, and hardware security protocols.

4. Privacy and data protection risks

The privacy risks associated with personal data being collected by data controllers are not a new phenomenon. However, the data privacy implications associated with apps are heightened beyond traditional data collection means because of apps' ability to collect data instantaneously, continuously, and often without knowledge of the user, at an extremely granular level, whether it be the

[34] J. Chrétien and others 'Using Mobile Phone Data to Observe and Understand Mobility Behaviuor, Territories, and Transport Usage' in *Urban Mobility and the Smartphone* (Elsevier 2019) 82.

[35] See S Bu-Pasha, *Location Data, Personal Data Protection and Privacy in Mobile Device Usage: An EU Law Perspective* (Helsinki (2018); C Bettini, Privacy Threats in Location-Based Services (n. 25); Article 29 WP, Opinion 13/2011 n. 185 on Geolocation services on smart mobile devices https://iapp.org/media/pdf/resource_center/wp185_Geolocation-smart-devices_052011.pdf Accessed August 2019.

exact coordinates or the specific heart rate of an individual at any given moment. This micro-level collection of data by sensors creates more pressing data privacy implications for individuals.[36] On MaaS ecosystem the digital interface between users and MaaS provider is their smartphone and in an ideal workflow, after possibly having set their preferences, they send a request and receive in response one or more "mobility solutions", they pay the ticket for the one selected. Besides leaving aside that, matching the GPS coordinates other of the smartphone with its location, the system can track users in their route, allowing it to follow his/her movements in real-time and to detect a pattern. Since the preliminary analysis on Intelligent Transport System, the real possibility that the user could be not only profiled but also "singled out" has raised many concerns, which become more sensitive in MaaS due the increasing number of interconnected databases.[37] It is important to underline that by collecting location data, MaaS provider or app developers are able to deduce many types of personal information apart from merely location, such as religious believes or political affiliation. To give an example, if a person visits a church regularly or goes to a gay bar in the weekends, conclusions can be drawn about that person's religion or sexual preferences. Because many privacy-protected attributes are uniquely associated with places or events, collecting data that show a person frequently visits a place or attends a particular event represents a powerful means to draw a comprehensive picture of an individual.[38] In such cases, location data becomes special categories of personal data or "sensitive data", such information on the frequency and place of obtaining medical care, religious activities, political orientation or sex life, that require a higher level of protection under Art. 9 GDPR and in the case of sensitive data it prohibits its dissemination by default. Only under specific conditions might such data be processed. These profiles can be used to take decisions that significantly affect the owner. Moreover, other data can be inferred through the publication of location data, for example real-time emotional and physiological status[39], and co-location (i.e. the presence of other people in the same location). In a nutshell, two fundamental rights are in risk from collecting and processing location data: first the right to privacy and sec-

[36] A. Fong, *The role of app intermediaries in protecting data privacy*, in International Journal of Law and Information Technology (2017) 85-114.

[37] F. Costantini, MaaS and GDPR: an overview (2017), in https://arxiv.org/abs/1711.02950 Accessed August 2019

[38] S Bu-Pasha and others 'EU Law Perspectives on Location Data Privacy in Smartphones and Informed Consent for Transparency' in *European Data Protection Law Review*, *2*(3/2016) 312-323

[39] D. Riboni, L. Pareschi, C. Bettini, 'Privacy in location-based applications' in *Privacy in Georeferenced Context-Aware Services: A Survey*, (Springer-Verlag 2009) 151-172.

ondly the right to data protection. Generally, the right to privacy – referred to in European law as the right to respect for private life – emerged in international human rights law in the Universal Declaration of Human Rights (UDHR), adopted in 1948, as one of the fundamental protected human rights. Soon after adoption of the UDHR, Europe too affirmed this right in article 8 of the European Convention on Human Rights (ECHR). The right of data protection emerged as a need to control collection of personal data enhanced by digitalisation. The right to respect for private life and the right to the protection of personal data are closely related. Both strive to protect similar values, i.e. the autonomy and human dignity of individuals, by granting them a personal sphere in which they can freely develop their personalities, think and shape their opinions. They are thus an essential prerequisite for the exercise of other fundamental freedoms, such as freedom of expression, freedom of peaceful assembly and association, and freedom of religion.[40] The two rights differ in their formulation and scope. The right to respect for private life consists of a general prohibition on interference, subject to some public interest criteria that can justify interference in certain cases. According to Advocate General Sharpston[41], the protection of personal data is viewed as a modern and active right putting in place a system of checks and balances to protect individuals whenever their personal data are processed. In regard to location data privacy, according to Alastair R. Beresford and Frank Stajan[42] definition it's "the ability to prevent other parties from learning one's current or past location". Location data privacy implies the right to not be subjected to unauthorised collection, aggregation, distribution or selling of an individual or organization's location or location profile derived from location data.[43] The concept of location data privacy does not refer to hiding information – rather it safeguards one's present or past location information from use for commercial or other purposes without one's knowledge. In connection with location data, when a person loses the ability to control his or her location information, or the ability is limited somehow by another authority, that person's privacy came under threat.[44] Considering privacy principle, it is neces-

[40] Handbook on European data protection law, 2018 edition, https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law Accessed August 2019.

[41] Advocate General Sharpston, see CJEU, Joined cases C-92/09 and C-93/02, Volker und Markus Schecke GbR v. Land Hessen, Opinion of Advocate General Sharpston, 17 June 2010, para. 71.

[42] R Alastair, Beresford, F Stajano, 'Location privacy in pervasive computing' in *IEEE Pervasive Computing*, 2(1): 46–55, 2003 Available online here https://www.cl.cam.ac.uk/~fms27/papers/2003-BeresfordSta-location.pdf.

[43] Location Forum, *Location Data Privacy Guidelines* (n. 30) 7.

[44] S. Bu-Pasha, *Location Data, Personal Data Protection and Privacy in Mobile Device Usage (n. 34) 9.*

sary to take into account participants' perception and behaviour surrounding their privacy. The "privacy paradox," which designates the fact that people declare concern for their personal information but willingly diffuse it online also applies to geolocation technologies [45] which explains the broadness of data currently available. However, this is not to say that individuals "give away" their information or location randomly: they are more likely to accept to relinquish some privacy if the website or application is entertaining, provides monetary or social benefits. [46]

5. Personal location data under GDPR

The EU's General Data Protection Regulation (GDPR) aims to change the way that consumer data is gathered and used. The GDPR applies to any processing of personal data which means any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means (Art. 4 n. 2 GDPR.) However, data has to be personal in order to fall within said scope of application of the Regulation. Data is deemed personal if the information relates to an identified or identifiable individual, (Art. 4 n. 1 GDPR.) Article 4 of the GDPR recognize location data expressly as a factor by reference to which a person may be directly or indirectly identified, thus is recognised as personal data if they identify a natural person. In order to understand the role of location data under GDPR, it is important to distinguish between cases where location data constitute either personal data or sensitive data from those cases where the data are effectively anonymised, thus not considered personal data and GDPR does not apply. [47] As a personal data, the following provisions of GDPR are applicable to location data privacy. Article 5 of the GDPR states the principles to be followed in in processing personal data. The GDPR introduces the general principle of accountability in Art. 5 Sec. 2 GDPR, which imposes the responsibility for the compliance of processing with the GDPR and

[45] A.M. Zafeiropoulou, (2014) *A Paradox of Privacy: Unravelling the Reasoning Behind Online Location Sharing* (Ph.D)University of Southampton https://eprints.soton.ac.uk/376477/1/_userfiles.soton.ac.uk_Users_slb1_mydesktop_soton.ac.uk_ude_personalfiles_users_jo1d13_mydesktop_Zafeiropoulou.pdf Accessed August 2019.

[46] S Kokolakis, 'Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon' in *Computers & Security* 64 (2017) 122-134 https:// doi.org/10.1016/j.cose.2015.07.002 Accessed September 2019.

[47] P Voigt, & A Bussche, *The EU General Data Protection Regulation (GDPR) Handbook*, (Springer 2018) 13; Same position also, S Bu-Pasha, *Location Data, Personal Data Protection and Privacy in Mobile Device Usage (n. 34) 64.*

the burden of proof for said compliance into the controller (Voigt & Bussche, 2018). Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (Art. 5 Sec. 1. a). Entities should first decide on the purpose of collecting data and then, by notifying the data subject about the purpose, collect data only to fulfil that purpose. Personal data shall only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (Art. 5 Sec. 1. b). Thus, it restricts the secondary use of data. For instance, LBS app, like MaaS and Google Maps collect location data offering particular geographical location services. The GDPR makes it clear that location data collected for a particular purpose should be used for its declared purpose only. [48] Therefore, data processor or controller on MaaS cannot use that data for advertisement or any secondary purpose without an additional consent from data subject. In addition, Art. 5. (c) of GDPR establish the data minimisation principle, aiming for a reduction of data collection to the lowest possible level for realising the processing purposes by companies. According to the "storage limitation" principle in Art. 5 (f) personal data can be stored "no longer than is necessary for the purpose for which the personal data are processed". Moreover, Art. 6 of GDPR has strengthened the conditions of data processing such that processing is permitted only when it's necessary on lawful grounds.

Further concrete data protection instruments are being prescribed in Art. 25 GDPR: companies should use the concepts of Privacy by Design and Privacy by Default. It means that entities and organizations should adopt appropriate technical and organizational measures from the beginning of the service. Privacy by Design (Art. 25 Sec. 1 GDPR) is based on the realisation that the conditions for data processing are fundamentally being set by the soft and hardware used for the task. When creating new technology, developers and producers shall be obliged to keep data minimisation in mind. However, data protection by design is about complying with GDPR as a whole and the most effective way of discharging the controller's burden of that compliance is to avoid processing personal data in the first place, like pseudonymisation. [49] On the other hand, the concept of Privacy by Default (Art. 25 Sec. 2 GDPR) shall protect consumers against the widespread trend among companies to obtain as much personal data as possible. [50] By default, only personal data that are necessary for the specific

[48] Bu-Pasha, *Location Data, Personal Data Protection and Privacy in Mobile Device Usage (n. 34) 38.*

[49] For more information see D Kelleher, M Karen, EU Data Protection Law (Bloomsbury Professional 2018)267.

[50] P. Voigt, A Bussche, *The EU General Data Protection Regulation* (n. 46) 63

purpose of the data processing shall be obtained. Where users wish to change settings of a service, e.g. to allow further use of or share their personal data with more parties, they should have to opt in and amend the settings by themselves.

Data subject has under GDPR a set of rights over his or her data. According to the Handbook on European data protection law[51] first of all, controllers of processing operations are obliged to inform the data subject at the time when personal data are collected about their intended processing. As data processing can negatively impair the rights and freedoms of data subjects, especially where it is unlawful or where it involves incorrect or incomplete data, the GDPR provides for different rights of data subjects that permit them to limit or influence processing activities carried out by the controller. These rights are the right to rectification, the right to consent, the right to erasure and the right to restriction of processing. Article 20 GDPR introduces a new data subject right, the right to data portability which is the right for customers to transfer their data from one data system to another and is extremely important for MaaS. According to Transport Systems Catapult[52] this means that customers can switch MaaS providers encouraging a competitive market which supports innovation, quality assurance and the delivery of value for money. The GDPR also outlines the responsibilities of data holders such as the responsibilities to encrypt and anonymise data, report data breaches, and record processing activities.

5.1. Sensitive location data

Generally, location data are not sensitive but can disclose sensitive information in association with other information, tending to become sensitive data under EU data protection law[53] (Bu Pasha, 2018) with special legal effects (Art. 9 GDPR). Those special categories of personal data merit specific protection as they allow conclusions about an individual that are linked to his fundamental rights and freedoms, and their processing might entail high risks for the latter. Deducing user's sensitive patterns (data) on MaaS is easier whenever data location is combined with user's ID name, email address, telephone number, physical address, account number, credit cart, which are identifying personal data.

[51] *Handbook on European data protection law*, (n. 39) 111.

[52] Transport Systems Catapult (2016). Mobility as a Service: Exploring the opportunity for Mobility as a Service in the UK [Online] Available at: https://ts.catapult.org.uk/wpcontent/uploads/2016/07/Mobility-as-a-Service_Exploring-the-Opportunity-for-MaaS-in-the-UK- Web.pdf Accessed August 2019

[53] Bu-Pasha, *Location Data, Personal Data Protection and Privacy in Mobile Device Usage (n. 34) 47.*

Moreover, the risk increase considering that MaaS app access phone's identifiers, such as International mobile equipment identity and Identity management system, which, as shown by Enck [54], are among the most commonly used sensitive data that app collects. One of the reasons why MaaS provider needs to have such personal data is because some tickets or monthly subscriptions are personalized and valid only for special type of users. (i.e. student card). Location data on MaaS are highly valuable to a number of interested parties with diverse intentions and purposes, ranging from advertisers to car manufacturers, transport operators and public transport management authorities. For instance, in order to avoid traffic jams transport authorities can develop models to forecast how user travel in time and space, and to understand the factors that influence on travel-related choices. However, unrestricted and indiscriminate access to data shared may allow for the unfair accumulation of individual movement profiles, a "datification" of pattern behaviours on which personalized goods and services can be shaped, advertised and sold [55] (WP29 n. 252, 2017). From a GDPR point of view, it's not clear for example how data concerning trips to hospitals (or to other sensitive places) could be lawfully treated in MaaS, since they would qualify as "data concerning health" by Article 4 n. 1 (15) of GDPR and they would fall into the prohibition of Article 9 n.1 of GDPR. Considering that MaaS could identify user's sensitive patterns, whenever monitoring a user's travel destination through location data which may reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic data or biometric data, data concerning health or data concerning a natural person's sexual orientation processing shall be prohibited by default under Art. 9 of GDPR. Nevertheless, the provision introduces several exceptions from the prohibition of processing special categories of personal data (i.e. consent of data subject). Data subject can explicitly consent to the processing of special categories of personal data for one or more specified purposes. Such affirmative act not only has to fulfil the general conditions for valid consent under Arts. 7, 8 GDPR but also has to explicitly refer to the special categories of personal data concerned by the intended processing. [56]

[54] W. Enck, D. Octeau, P. McDaniel, S. Chaudhuri, 'A Study of Android Application Security' in *Proceedings of the 20th USENIX Security Symposium (USENIX Security 2011)*, 1-16.

[55] Article 29 WP, n. 252, (10/2017) Guidelines on Processing personal data in the context of cooperative Intelligent Transport System https://ec.europa.eu › newsroom › just › document Accessed August 2019, 8.

[56] P. Voigt, A. Bussche, *The EU General Data Protection Regulation* (n. 46) 112.

5.2. Legal justifications for location data processing

Article 6 of GDPR sets the conditions for a lawful personal data processing and describes six lawful bases on which a controller can rely. The application of one of these six bases must be established prior to the processing activity and in relation to a specific purpose. [57] Different roles are involved in the processing of personal data. A controller defines the purposes and methods of processing personal data, independently or together with others (Art. 24 GDPR). A processor processes personal data on behalf of the controller. In this case, processing is commissioned or subject to subcontracting or a partnership (Art. 28 GDPR). There can also be parallel controllers, in which case each controller has an independent right to process personal data (Art. 26. GDPR). The processor does not have any independent right to use the data. The controller must notify data subjects of any processing of personal data. This information includes the controller's contact details, information about the purpose and principles of data processing, and information about the rights of the data subjects. (Art. 13 GDPR). The provider of a MaaS application that is capable of processing geolocation data is the controller for the processing of personal data resulting from the installation and use of the application, independently from the developer of the operating system and/or the controllers of geolocation. Basically, any treatment of data will be considered as processing. Examples include collecting, recording, organising, structuring, storing and erasing of data.

A common regulatory challenge around transport platforms is to define their legal status which may also reflect the roles involved in the processing of personal data. In particular, the debate has focused on whether they provide an intermediation service using digital technology, or they really provide a full transportation service, for which a license is often required, and full liability before passengers has to be ensure. This has been the case of Uber considered by European Court of Justice as transport provider instead of mere intermediary service. [58] In MaaS ecosystem, the MaaS operator, being the transport provider, acts as the controller regarding personal data collected from passengers. On the other hand, the MaaS operator being the intermediary, and transport service providers can act as controllers and/or processors, depending on which data is being processed and what has been agreed upon regarding the tasks and roles of

[57] Article 29 WP n. 259, 12/2017 on Guidelines on Consent under Regulation 2016/679 http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849 Accessed September 2019

[58] See J. Montero, 'Regulating Transport Platforms: The Case of Carpooling in Europe' in M. Finger, M. Audoin, *The Governance of Smart Transportation Systems* (Springer 2019) 11-25

each party. Deviating from any roles defined in legislation is not possible. Generally, for MaaS provider with regard to the legal basis for data processing, three different possibilities seem to be more suitable to be applied [59]: Art. 6 (1) (a) of GDPR (consent by the data subject), Art. 6 (1) (b) of GDPR (performance of a contract) or Art. 6 (1) (f) of GDPR (legitimate interest). In specific, Bu Pasha (2018) in her work had considered consent as the easiest way to process location data through, on one hand, providing notice of the users about the way, extent and possibility of collection and processing of their location data, on the other hand, seeking their consent. Therefore, whenever processing of (patterns of) location data is based on consent, the MaaS data controller shall be able to demonstrate that the data subject has consented to the processing, (Art. 7. Sec. 1 GDPR). Thus, it bears the burden of proof, for example, if a data subject claims to have given no or no valid consent, which corresponds to the controller's accountability under Art. 5 Sec. 2 GDPR for the lawfulness of data processing. Article 4(11) of the GDPR defines consent as: *"*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.*"* Consent is presumed not to be freely given if the consent does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case. [60] Every new and different use of location data not covered under the introductory notice should provide separate notice to the users asking their consent. [61] For example, whenever location data become sensitive data, a separate and different user's consent should be obtained. Under EU law, article 7(3) of the GDPR prescribes that the controller must ensure that consent can be withdrawn by the data subject as easy as giving consent and at any given time. The data subject must be informed of such a right prior to giving consent and he or she may exercise this right at his or her discretion. There can be no free consent if the data subject is unable to withdraw his or her consent without detriment or if withdrawal is not as easy as giving consent had been. [62] As a general rule, if consent is withdrawn, all data processing operations that were based on consent and took place before the withdrawal of consent remain lawful, however, the controller must stop the processing actions concerned. If there is no other

[59] F. Costantini, E Archetti, B Ferencz and F Di Ciommo, (2019) *Iot, intelligent transport systems and MaaS*, in https://cambiamo.net/publicaciones/iot-intelligent-transport-systems-and-maas-mobility-as-a-service/ Accessed August 2019, 5.

[60] P. Voigt, & A. Bussche, The EU General Data Protection Regulation (n. 46) 94.

[61] See again Bu-Pasha, *Location Data, Personal Data Protection and Privacy in Mobile Device Usage (n. 34) 38.*

[62] Handbook on European data protection law, (n. 39) 150.

lawful basis justifying the processing (e.g. further storage) of the data, they should be deleted by the controller. [63]

5.3. Data Privacy Impact Assessment (DPIA)

MaaS provider is the owner of the technological platform where different datasets converge, and to which all customers address their demand. Among the many duties of this agent, two are worth mentioning because they are imposed in order to foster information security. [64] The first is the Data Protection Impact Assessment (DPIA) that has to be performed before starting the "processing" because MaaS can be defined as "*a systematic monitoring of a public accessible area on a large scale*" (Article 35. 3 (c) GDPR). The second is the obligation to notify a personal data breach to the supervisory authority within 72 hours (Article 33. 1 GDPR) and to the data subject "without undue delay" *ex* Article 34 .1 of the GDPR. Moreover, MaaS provider may be "*processing on a large scale of special categories of data referred to in Article 9(1)*" (Article 35. 3. (b) GDPR) or in *a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling…* (Article 35. 3 (a) GDPR). Therefore, location data enforce the need of a DPIA on MaaS, having a central role in the above hypothesis because they are fundamental to monitor traveller's behaviours, they become sensitive in combination with other data and they could help MaaS provider to categorize its users.

DPIAs are important tools for accountability. [65] This new tool of the GDPR is highly relevant for any processing of personal data, as it helps to structure the process, be aware of data protection issues and the relevant legislation and implement proper safeguards to protect data subjects. DPIA begins before any data are processed and continues throughout the life cycle of a project and its data processing operations. At the heart of this process is the analysis of high risks to the rights and freedoms of individuals that may emanate from the processing of personal data and is the basis for mitigating these risks through technical and organisational measures. A DPIA must be undertaking by the controller who must first consider who will he ask to actually do the work of carry a DPIA on

[63] See Article 29 WP n. 259, 12/2017 (n. 56) 22.

[64] F. Costantini, MaaS and GDPR (n. 36) (2017).

[65] Article 29 WP n. 248, 4/ 2017 on guidelines on DPIA and determining whether data processing is likely to result in a high risk for the purpose of regulation 2016/679 https://ec.europa.eu /newsroom/article29/item-detail.cfm?item_id=611236. Accessed September 2019, 4.

his behalf. [66] If the DPIA finds that the risks to the rights of individuals remain high even with the identified measures, the controller has to consult the Supervisory Authority according to Article 36 GDPR before the processing can start. The controller may also decide to abandon the processing operation. It's clear that the GDPR requires a very broad analyse of the risk posed by a processing operation. The Article 29 of Data Protection Working Party on guidelines on DPIA suggest that there must be a consideration of all risks to rights and freedoms not just data protection rights. Whenever a controller concludes that the operation in question is not high risk it will want to retain a record of that assessment, so that it can demonstrate compliance with its obligation to consider article 35 GDPR. If the controller does not undertake a DPIA in circumstances where the Supervisory Authority concludes one should have been done then a fine up to 2 per cent of global turnover may be imposed (Art. 83 (4) (a) GDPR). If a DPIA has not been done then the Supervisory Authority could order than one be done in a specific manner and within a specific period (Art. 58 (2) (b). and it may limit or ban the controller from processing personal data in the meantime. (Art. 58 (2) (f) GDPR.) Moreover, data subjects may ask compensation for material or immaterial damage that they have suffered as a result of processing undertaken in the absence of a DPIA (Art. 82 GDPR).

5.4. Anonymization and Pseudonymization Location Privacy

In DPIA anonymisation techniques and pseudonymization could be considered as means of securing user identity. The WP 29 suggest that anonymisation techniques can provide privacy guarantees and may be used to generate efficient anonymisation processes, but only if their application is engineered appropriately – which means that the prerequisites (context) and the objective(s) of the anonymisation process must be clearly set out in order to achieve the targeted anonymisation while producing some useful data. The optimal solution should be decided on a case-by-case basis, possibly by using a combination of different techniques. [67] In anonymised data, identifiable elements are irreversible destroyed in order to achieve irreversible deidentification of data subject. Pseudonymization substitutes the identity of the data subject in such a way that additional information is required to re-identify the data subject. With the advent of GDPR it is important to understand the difference between anonymized data

[66] D Kelleher, M Karen, *EU Data Protection Law* (n. 48) 269.

[67] Cfr Article 29 WP, Opinion 5/2014 n. 216 on Anonymization techniques https://www.dataprotection.ro/servlet/ViewDocument?id=1085 Accessed September 2019, 3

and pseudonymized data since the former are not considered as personal data. [68] In contrast, identifiable elements, are replaced by pseudonyms with which data subject cannot be directly identified, but identifiable data are reversible. The Working Party [69] (2014) emphasizes that there are two different approaches to anonymisation: the first is based on randomization while the second is based on generalization. Randomization is a family of techniques that alters the veracity of the data in order to remove the strong link between the data and the individual. If the data are sufficiently uncertain then they can no longer be referred to a specific individual. Randomization may protect against inference attacks/risks and can be combined with generalization techniques to provide stronger privacy guarantees. Otherwise, generalization consists of generalizing, or diluting, the attributes of data subjects by modifying the respective scale or order of magnitude (i.e. a region rather than a city, a month rather than a week).

Art. 4(5) GDPR introduce pseudonymization on a legal basis, which implies separating the identifying elements of personal data by pseudonyms. [70] Pseudonymization is mentioned as "an appropriate technical and organisational measures" for data protection and data minimization in Art. 25. (1) of the GDPR. For instance, obfuscation can be practical way for users to protect their location when engaging in LBSs. Instead of using their accurate location *x*, users employ a Location Privacy Protection Mechanism (LPPM) that computes a pseudo-location *z* and then transmits this pseudo-location to the service provider. As a result, the LBS provider and third parties receive only altered or approximate location instead of accurate location information. According to Herrmann [71] (2016), there are four main types of obfuscation strategies that have been extensively studied in the literature:

a) hiding location data: with this obfuscation strategy the user stops engaging in the LBS for a certain time or at a certain place;

b) perturbation: a user may perturb her location, i.e. use the library as her current location instead of her true location the hospital, in order to protect her location privacy;

c) reducing precision: instead of using accurate locations, the user provides

---

[68] Both scholars share the same position, P. Voigt, A. Bussche, *The EU General Data Protection Regulation* (n. 46) 13; S Bu-Pasha, *Location Data, Personal Data Protection and Privacy in Mobile Device Usage (n. 34) 64.*

[69] Article 29 WP, Opinion 5/2014 n. 216 on Anonymization (66) 11.

[70] C Williamson, 'Pseudonymization vs anonymization and how they help with GDPR' in https://www.protegrity.com/pseudonymization-vs-anonymization-help-gdpr/ Accessed September 2019.

[71] M. Herrmann, 'Privacy' in Location Based Service (2016), in https://www.esat.kuleuven.be/cosic/publications/thesis-273.pdf Accessed August 2019, 55-63

a cloaking region to the LBS provider. For example, a user provides as location the region of a city instead of her accurate GPS coordinates;

d) and dummies: a dummy based LPPM queries the LBS with a series of fake locations that may include the user's actual location *x*. If the LBS accepts dummy queries, the LPPM can send the set of locations directly to the LBS and receives in return an answer to every location in *z*.

Another practical and safest way to protect location data is the recent practise adopted by Google [72] (2019) which now let's user to automatically delete location and activity history. However, latest research indicates that anonymization and pseudonymization are not sufficient at preserving the security of the data. An example that shows the potential of location data in de-anonymisation is the experiment conducted by De Montjoye. [73] They showed that with a dataset of location data they could uniquely identify 95% of the people in a large anonymised data set (approximately 1.5M users of a mobile phone operator). Confirming the previous Bettini's research [74] which showed that anonymization of location traces of a person is hardly possible because the traces of users are a spatiotemporal pattern that is almost unique to each user. Therefore, pseudo-anonymization does not offer any protection of user traces, because the pseudonym allows to reconstruct user traces.

6. Conclusions

Based on the value of location data, LBSs has risen. The importance of LBSs are undoubtful, however alongside the benefits, location data privacy vulnerabilities has been subject of concerns by scholars. As showed in section (5.1), on MaaS personal location data could become easily sensitive data in combination with other information. Processing data of the MaaS end-user and the improper use of sensitive data related to pattern trips are important legal concerns. Therefore, unlawful and unfair interference with location data has a direct nega-

[72] Mathew Katz (June 2019) Google will now let you auto-delete your location history, https://www.digitaltrends.com/android/google-automatically-delete-location-history/Accessed November 2019; See also, John Moreno (June 27, 2019) Google will now let you automatically delete location and activity history. Here's how https://www.forbes.com/sites/johanmoreno/2019/06/27/google-can-now-automatically-delete-your-location-data-heres-how/ Accessed November 2019

[73] Y.A. De Montjoye and others, *Unique in the Crowd: The privacy bounds of human mobility* (Scientific reports 2013) 1376.

[74] C. Bettini, C.X. Sean Wang, S. Jajodia, 'Protecting Privacy Against Location-Based Personal Identification' in *Second VLDB Workshop on Secure Data Management (SDM*, volume 3674 of *Lecture Notes in Computer Science* (Springer Berlin Heidelberg 2005) 185-199.

tive impact on privacy, which has a significant effect on the private lives of smartphone users and also of other individuals. In order to secure and protect the location data and privacy of smartphone users from unauthorised access, use, disclosure or retention, some administrative, regulatory and technical procedures are required. However, in such cases, and in many others, it seems that the guarantees provided by GDPR, either strictly legal (such as the consent of the data subject [Article 7 GDPR]), or technological (such as "Privacy by Design" [Article 25 GDPR]) are not suitable to avoid the risk that the "controller" or the "processor" could be punished accordingly. [75] Subsequently, bedside the guarantees and sanctions in case of data breach offered by GDPR, in order to fully protect personal location data privacy, more information and education about the risks, the values and opportunities emerging from personal data should be promoted by Supervision Authorities to the data subjects. In other words, a reciprocal cooperation will reduce the risk of unlawful and unfair processing of personal location data.

[75] F. Costantini and others, *Iot, intelligent transport systems and MaaS* (n. 58) (2019) 9.