MaaS Surveillance: Privacy Considerations in Mobility as a Service

Caitlin D. Cottrill

Centre for Transport Research, Department of Geography & Environment, School of Geosciences, University of Aberdeen

Abstract

The concept of Mobility as a Service (MaaS) is seeing increasing attention from researchers, industry, and the public sector. MaaS, which posits that traditional models of car ownership and travel may be supplanted by models focused on packages of shared vehicle access, use of public transport, active transport, and teleworking, is currently viewed as having potential beneficial impacts including reductions in single-occupancy vehicle trips, with concomitant reductions in travel cost, congestion, and environmental concerns. MaaS, however, relies upon a number of social expectations, including trust, reliability, and transparency, each of which is reliant upon both the social network that enables MaaS to work efficiently, and upon the ways in which data are handled within the enabling framework. In light of this, it is anticipated that the recently-enacted General Data Protection Regulation (GDPR) has the potential to significantly impact upon the further implementation of MaaS. MaaS services are predicated upon the sharing of personal travel information (vehicle availability, origins, destinations, financial information, social network data, etc.) that, under GDPR, may be considered personal, subject to the regulations and restrictions this categorisation implies. For MaaS to work in a European context, then, it must be responsive to GDPR requirements related to issues such as Privacy by Design, Consent, and Protection. In this paper, we explore the concept of MaaS in relation to privacy considerations raised by GDPR requirements, with attention to methods and techniques related to relevant data acquisition, sharing, and protection processes. A case study of the Whim application's privacy policy is presented to demonstrate the potential implications of this policy in an applied context.

Introduction

The concept of Mobility as a Service (commonly referred to as MaaS) is seeing increasing attention from researchers, industry, and the public sector in keeping with heightened expectations for personal mobility and rising concerns for the environmental health of urban spaces. MaaS, which posits that traditional models of car ownership and individual trips may be supplanted by models focused on packages of shared vehicle access, use of public transport, active transport, and teleworking, is currently viewed as a new way forward, with potential beneficial impacts including reductions in single-occupancy vehicle trips, with concomitant reductions in cost to individuals, congestion, air pollution, and surface runoff from parking pavement. While the potential for such benefits is great, however, realising them is contingent upon ensuring that MaaS systems are responsive to end-user expectations and that the underpinning technology and data platform are acceptable to service providers. A particular area that is of relevance and interest to both end users and service providers is that of data privacy.

Effective MaaS systems are reliant upon both the social networks that enable them to work efficiently and capably, and upon the way in which data are handled within their enabling frameworks. While the providers of MaaS services cannot guarantee that every user will behave in accordance with the regulatory guidance that they set forward, they can develop user systems that encourage good behaviour and minimise potential negative impacts in the spirit of meeting the necessary expectations. While the importance of addressing privacy considerations in this context has been raised in a number of publications, including Jittrapirom et al. (2018), which identified privacy as a potential constraint to meeting MaaS objectives, it has not yet been comprehensively addressed with respect to the underlying privacy considerations raised by extensive access to identifiable location data, with potential distribution across multiple service providers.

In light of this, it is anticipated that the current privacy concerns addressed by the recently enacted European General Data Protection Regulation (GDPR) has the potential for significant impacts upon the further implementation of MaaS. MaaS services are often predicated upon the sharing of personal information related to travel: vehicle availability, current origin, planned destination, financial information, social network data, and others. Under GDPR, this data may be considered personal, and is subject to the regulations and restrictions this categorisation implies. For MaaS to work in a European context, then, it must be responsive to GDPR requirements related to issues such as Privacy by Design, Consent, Protection, and Security. It must, in short, respond to an environment that both demands data revelations and protects them. In this paper, we explore and examine privacy issues in the provision of Mobility as a Service systems, and how these may relate to the General Data Protection Regulation (GDPR). We review a case study example of a MaaS-related privacy policy for the WHIM app that is response to the GDPR, in order to demonstrate the various considerations that GDPR requirements demand of MaaS service providers. We hope that the paper will serve both to establish a baseline understanding of the implications of the GDPR for MaaS providers and projects, and a proactive method for ensuring that emerging projects benefit from the trust and security enhancements anticipated from an increased focus on data protection.

In this paper, we begin by introducing the place of privacy and security in the transport context, followed by a detailed overview of Mobility as a Service and expected impacts on its feasibility under the General Data Protection Regulation (GDPR). This will be followed by a more robust discussion of potential methods currently under consideration for responding to GDPR requirements, and an overview of an example policy reflective of GDPR considerations. The review of the Whim application's privacy policy provides an example of how current MaaS service providers are

responding to requirements imposed by the GDPR, and how this may impact upon their treatment of consumer data, and how that treatment is communicated to the user.

Privacy and Security in the Transport Context

In the Ministerial Forward to the Public Consultation for the Security of Network and Information Security Directive, the Rt Hon Matt Hancock (Minister of State for Digital) wrote, "Our modern economy, and the economic security it brings, are all themselves based on secure infrastructure. Network and information systems and the essential services they support play a vital role in society, from ensuring the supply of electricity, water, and health services, to provision of passenger and freight transport (P.4, 2017)." The inclusion of passenger and freight transport in this list underscores the critical role that the sector plays in the functioning of a stable, economically sound society. In addition, the recognition of transport as sitting within a network context highlights the diversity of interests involved in the transport context – from users and passenger service providers, to infrastructure for physical and information services, to freight and logistics interests.

For the network to function efficiently, however, and to best serve the interests required of it, modern transport systems rely on robust data sources, collected from a wide variety of providers, and used for a number of different purposes. Some of these sources may include the following, as defined by George et al. (2014):

- Data: Data typically held by governments, governmental organizations or local communities. These data are generally available for widespread use, and may include Census and transport data, or energy use.
- Private Data: Data acquired and held by private firms, third sector organisations or individuals. These data can generally not be obtained via public source data resources and may include proprietary information such as mobile phone usage, data from RFID tags, or data on freight movements.
- Data Exhaust (or passive data): 'Ambient' data, passively collected and not core to the specific activities of the collecting agency. While of limited value as standalone data sets, they are often useful when combined with other data sources. Such data may include internet search histories, location traces from mobile phones, or interaction records.
- Community Data: Unstructured data captured, for example, as part of social interactions, such as online reviews/ratings, or social media feeds (such as Twitter or Facebook). These data can be analysed and structured to infer meaningful patterns (e.g., Cottrill et al., 2017).
- Self-Quantification Data: Data revealed by individuals through self-monitoring or tracking, such as through the use of personal fitness trackers.

Actors in the transport realm are increasingly making use of combinations of these data sets for service provision, project and network planning, modelling, and programming (Zhao et al., 2015; Cottrill and Derrible, 2015; Çolak et al., 2015). Pigni et al. (2016), for example, cite the example of Uber, which "…owns no vehicles, but harnesses a real-time digital data stream of its drivers' cars and matches them with real-time demand for rides (p. 5)." Zheng et al (2016), in turn, indicate a number of examples of the use of multiple forms of data for transport projects, including cell phone and WiFi data; social media data from Facebook, Twitter, Waze, and other social media services; incident reports; and location-enabled web logs, such as Foursquare. They note that, "In terms of data contents, social transportation data record Time, GPS coordinates, Velocity, Accelerated Velocity, Address, Texts, Video etc. For each type of social transportation data, the recorded contents are specific to one or several aspects of human mobility, and specific to information of a person or a

community (p. 621).” Such a variety of data sources and uses, as well as the identification of the likely specificity of this to individual actors, provides a sense of the scope of privacy concerns emerging in the current transport ecosystem.

Given the multiplicity of actors involved in the collection and use of relevant data, including government agencies, academic and research organisations, commercial entities, and third-sector organisations, the landscape for collection and handling concerns such as privacy and security may be inconsistent or fragmented (Jagadish et al., 2014; Patire et al., 2015; Goşman et al., 2016). In particular, the increasing spatial disaggregation of services through which data may be generated and collected (for example, Twitter is headquartered in California, USA, but its services are accessible worldwide, with data storage centres likewise distributed worldwide (Hashemi, 2017)) introduces additional complexity into the regulatory landscape, as multiple geographic scales may need to be considered. The use of cloud computing for storage or transmission of data used in transport applications is a useful case, as these may be domestic or cross-border. According to Svantesson and Clarke (2010), “…extraterritorial application of privacy laws risk being ineffective due to the difficulties associated with cross-border enforcement…[T]he simple fact is that today, it is extremely difficult for victims of privacy violations to obtain redress where the violation has occurred outside the victim’s home country (p. 393).” In such situations, consumers may be unclear as to the extent to which their data are protected, or the geographic extent to which that protection applies. Such considerations may, in turn, impact upon both the usefulness and completeness of data sets due to lack of consumer understanding or trust, evidenced by modifying privacy settings or providing false data (Keith et al., 2013; Wu et al., 2014).

Such issues of privacy and security are critical in the transport realm, as geotagged or otherwise location-enabled data represent valuable inputs into the transport data ecosystem (Buckley and Lightman 2015; Kitchin 2014). However, location data collected from personal devices or aligned to identifiable individuals can also be highly revealing, as it can be used to create detailed traces of an individual’s behaviour over time (Freudiger et al, 2011; Andrienko et al. 2013). According to de Montjoye et al. (2013), “…in a dataset where the location of an individual is specified hourly, and with a spatial resolution equal to that given by the carrier's antennas, four spatio-temporal points are enough to uniquely identify 95% of the individuals (p. 1).” Such findings indicate the extent to which location data, particularly in combination with other types of data as indicated above, may cast strong doubt on an individual’s right to privacy or expectation of security. While actions may be taken by the user (such as turning the device off or disabling location tracking) or the data collector (such as aggregating data or removing individual identifiers) to minimise the risk of privacy disclosure, such actions are not foolproof. In addition, taking such actions may also impact negatively upon the functionality of location-based services, which require detailed location information (often combined with personal preferences, habits, or social networks) to work most efficiently.

Introducing the MaaS context

The MaaS Alliance describes Mobility as a Service as, “…the integration of various forms of transport services into a single mobility service accessible on demand. 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 or car rental/lease, or a combination thereof. For the user, MaaS can offer added value through use of a single application to provide access to mobility, with a single payment channel instead of multiple ticketing and payment operations (MaaS Alliance, n.d.).” Kamargianni et al. (2016) further develop the underlying expectations of MaaS by identifying three main elements that are needed within MaaS systems to provide users with seamless journeys, including:

- *"Ticket & Payment integration*: when one smart card or ticket can be used to access all the modes taking part in the service and one account is charged for the use of those services;
- *Mobility package*: when customers can pre-pay for a specific amount (in time or distance) of a combination of mobility services;
- *ICT integration*: when there is a single application or online interface that can be used to access information about the modes (p. 3295)."

These elements, which highlight the importance of both service integration and the place of technology in facilitating access to MaaS, underscore the critical place of data and its' uses within MaaS service provision. An additional layer is added by Kamargianni and Matyas (2017) when they look more closely at the 'business ecosystem' underlying MaaS, which they classify into three layers: the core business layer, which comprises the MaaS provider, transport operators and customers; the extended enterprise layer, which consists of more technical firms, such as those providing back-end technical service, and payment and journey planning services; and the business ecosystem, which includes regulators and policy makers, researchers, unions, media and marketing firms and others (Kamargianni and Matyas, 2017). The multiplicity of identified involved interests further illustrates the complexity of the regulation of MaaS services.

In addition to this ecosystem of actors involved with providing MaaS services, it is generally expected that the mechanisms that will allow MaaS offerings to take place will be built upon easily-accessible platforms, likely available via, for example, a smartphone app. According to Jittrapirom et al. (2017), "MaaS relies on a digital platform (mobile app or web page) through which the end-users can access…all the necessary services for their trips: trip planning, booking, ticketing, payment, and real-time information. Users might also access other useful services, such as weather forecasting, synchronization with personal activity calendar, travel history report, invoicing, and feedback (p. 16)." The authors further identify the following as core characteristics of MaaS systems:

- Integration of transport modes
- Tariff option
- One platform
- Multiple actors
- Use of technologies
- Demand orientation
- Registration requirement
- Personalisation
- Customisation (Jittrapirom et al., 2017)

In addition to these overarching characteristics, Kamargianni et al (2016) have created an index that also looks at types of integration included in MaaS services, identifying four key areas that include: ticket integration, payment integration, ICT integration, and mobility package integration. The extent to which a MaaS service meets each of these types may have a substantial impact on the degree to which collected data may need to be shared among members of the business ecosystem, and, in turn, what expectations the user may have with respect to the likely use of provided data.

Meeting the needs of a fully integrated MaaS service that includes the core characteristics identified above will require the user to share a significant amount of personal information. To facilitate registration, some services (such as UbiGo) allow users to register via Facebook or Google, which improves convenience, but may bring into question to amount of data being shared between the MaaS service and the Single Sign On (SSO) system. While the use of SSOs is becoming more standard, Eagleman (2013) has found that, "…despite demonstrating a broad understanding of data

collection practices, users are unlikely to notice nuances, which we believe is due to habituation. Thus, improvements are needed to highlight data collection practices that are likely to diverge from users' expectations (p. 2369).” While such practices are useful for the service provider, as they provide a familiar platform for users and may allow access to certain useful profile information, they may also bring to the forefront questions of user data and its’ transferability. If a bespoke registration is required, this would likely consist of information that could further be used for personalisation and customisation of the service, thus requiring both standard registration information (such as name, contact information (email and phone number), and age and/or gender), as well as more targeted information (such as preferred travel modes and habits, access to a vehicle, presence or absence of a driving license, etc.). Further, the ability to schedule payment through the service will also necessitate that the user link his or her financial information, adding another layer of ‘static’ data to the profile.

When combined with time- and location-specific travel behaviour data needed to provide efficient services, these data have the potential to create a detailed portrait of travellers. Given that MaaS platforms may include both public and private service providers (with the potential of incorporating crowdsourcing for services such as shared rides or carpooling), access to these data sets will need to be carefully controlled in order to minimise privacy and security concerns. It is here where implications of the GDPR must be carefully considered.

Implications of the GDPR

The General Data Protection Regulation (GDPR, (EU) 2016/679), which was approved by the EU Parliament on 14th April 2016 and became fully enforceable as of 25th May 2018, replaced the EU’s Data Protection Directive (DPD - Directive 95/46/EC). Though some areas remain broadly consistent with the DPD, in many ways the regulation is responsive to the broad array of technological changes that have occurred in the past 20 years. According to the EC, “The aim of the GDPR is to protect all EU citizens from privacy and data breaches in an increasingly data-driven world that is vastly different from the time in which the 1995 directive was established. Although the key principles of data privacy still hold true to the previous directive, many changes have been proposed to the regulatory policies… (EUGDPR, 2017)” As with the DPD, the GDPR is applicable to personal data and sensitive personal data. The definitions of these have, however, changed somewhat – particularly that for personal data – in ways that have implications for the transport sector. Under the GDPR, personal data is defined as, “‘…any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, *location data*, an *online identifier* or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (GDPR, 2016; emphasis added).” The specific inclusion of both location data and online identifiers in this definition represents a change from the DPD, and has the potential to impact upon how MaaS services are offered and managed. Other key changes of the GDPR with the potential for impacting upon MaaS include the following:

- The GDPR increases the territorial scope of applicability, as it applies to all companies that process personal data of EU citizens, regardless of where the company is located.
- Requirements for obtaining consent have also been strengthened and place more onus on companies to provide consent language that is clear and easily accessible to the user. It must also be as easy to withdraw as to provide consent.
- The requirement to consider Privacy by Design has been codified into the regulation, which indicates that: “The controller shall…implement appropriate technical and

organisational measures...in an effective way…in order to meet the requirements of this Regulation and protect the rights of data subjects (GDPR, 2016)."

- Those data controllers and processors whose core activities consist of processing operations requiring large-scale, regular and systematic monitoring of data subjects or monitoring of special categories of data will be required to appoint a Data Protection Officer (DPO).
- Individuals are provided with the 'right to be forgotten', i.e. the user may request that the responsible data controller remove his or her personal data and cease any further dissemination of the data. This is also aligned with increased rights of the individual to obtain information on whether his or her personal data are being processed and, if so, where and for what purposes. (EUGDPR, 2017)

While this presents only in the broadest terms the areas of the GDPR that have the potential for implications on how MaaS services are provided and accessed, it is anticipated that other issues will emerge over time. For example, Costantini (2017) states, "…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. For example, it could be possible to find a pattern in a user's movements to and from healthcare facilities, and so correlate travels to certain diseases…in [which case] they would qualify as "data concerning health" by Article 4 §. 1 (15) of GDPR29 (p. 7)." Such concerns highlight the privacy issues inherent in the collection and monitoring of transport information over time, and the potential for them to reveal personal data.

The GDPR is applicable to data controllers and processors, defined in the regulation as follows:

- 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law; and
- 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller… (GDPR, 2016)

Under these definitions, it is evident that MaaS service provision will include both data controllers and processors, meaning that their activities will come under the scope of the GDPR. How considerations around the collection, sharing and processing of the types of data identified in the activities above will be addressed is, therefore, a timely and relevant question. This is further demonstrated in the amount of attention that the issue of GDPR in the transport sector has attracted from the legal sector. The Moovit app (https://moovitapp.com/), for example, published an updated privacy policy on the 21st of May, 2018 (immediately before full enactment of the GDPR), with the explicit statement that, "We have updated our Privacy Notice as part of our commitment to the high standard of data privacy protection introduced by the new European data protection law known as the General Data Protection Regulation (GDPR). Protection of your data and privacy has always been a top priority for us and that has not changed (Moovit, 2018)."

Some of the key areas of response that are relevant for MaaS practices are related to how data are obtained, accessed, shared, processed, and stored. Addressing these considerations in MaaS is further complicated by the multiplicity of actors involved – drawing together services from a number of providers and providing adequate data to make their practices efficient and accurate will require careful management of data streams, making sure that data practices are consistent, and establishing adequate security of personal information. The requirement for privacy by design,

defined as 'an approach to protecting privacy by embedding it into the design specifications of information technologies, accountable business practices, and networked infrastructures, right from the outset (Cavoukian, 2011)', would additionally impose the requirement that these considerations be made from the outset of the development of the MaaS project or consortium. Some of the key practices that should be codified in any MaaS agreement include the following:

- Development of consistent consent language that is clear and understandable, and adequately represents the underlying practices of relevant parties.
- Incorporation of Privacy by Design principles in the system architecture, particularly in instances where the sharing of data between processors is necessary for service provision or utilisation.
- Determine ways to minimise collection of data where possible.
- Establish consistent practices for users to request the removal of data, and methods of compliance across involved partners.
- Appoint a Data Protection Officer.

While these represent some initial steps that may be taken to ensure compliance with GDPR, it is evident that much scope for further evaluation remains.

Case Study: The Whim App

The Whim App was launched in the Birmingham, West Midlands area of England in April of 2018, following a previous rollout in Helsinki, Finland and with planned expansions in Greater Amsterdam in the Netherlands, the Antwerp region in Belgium, and Singapore by the end of 2018 (Intelligent Transport, 2018). According to MaaS Global, which has developed and launched the app: 'Whim makes mobility easier and seamless to West Midlands passengers in many ways:

- **All in one app:** Whim is the key to mobility. With just one click, you get access to National Express bus and metro tickets, routes and timetables and Gett taxis.
- **Travel your way:** Pay-as-you-go for multi-transport tickets with few clicks or get a monthly fixed-price package to cover all your daily journeys.
- **Plan travel in advance or go on a Whim:** Never miss the bus again. Whim syncs with your calendar and removes the hassle of travel planning. Also, get instant travel recommendations for spontaneous mobility with just a few clicks (MaaS Global, N.D.).'

The Whim privacy policy as of July 2018 was last updated on 24 May 2018 – the day before full enactment of GDPR. The policy itself reflects some of the core GDPR requirements as noted above, with particular attention to issues of comprehension (the policy scores a 12.6 Flesch-Kinkaid grade level, which correlates to a first-year university student, as opposed to an average of 14.6, or a second or third year university student, as found in Cottrill and Thakuriah (2011)) and observation of transparency regarding the collection of both personal and non-personal data. The policy (which is available online at https://whimapp.com/privacy/) provides a detailed overview of the types of data collected both through registration and through use of the app, including the following (MaaS Global, 2018):

- **Information collected directly from the consumer:**
    - ***Basic personal details:*** Most notably telephone number, which is requested when a user registers and acts as the account ID.
    - ***Additional personal details:*** These may include name, email address, and street address. Depending upon use of the app, this may also include information on

devices used, home country, language, credit card details and other payment details. It is noted that this information is needed to ensure that MaaS Global can process any payments made through the app. They also inform users that they use third party payment processors who will request and process details related to payments, which information will not be stored by MaaS Global. Third party log-in systems are also used, which may link Whim information with, for example, Facebook log-in and other information.

- ***Verification data:*** If necessary, Whim may at times require additional information such as personal identity number, photo, or driver's license details. This may be necessary if, for example, a car is being booked through the app.

- **Information collected through use of Whim services:**
  - ***Transaction information:*** Transaction records, including purchases, downloads, user-provided content, requests, agreements, services provided, delivery details and other interactions (including customer care) will be recorded and stored.
  - ***Positioning and location data:*** Whim makes use of location-based services, which establish the user's location through the use of satellite, mobile, Wi-Fi or other network based positioning methods. Location information gathered in these ways may be personally identifying, particularly if linked to a unique device, and may be shared with and stored by MaaS Global. Users are informed of the reasons for collecting this data, and are informed that it will not be used without consent.
  - ***Travel data:*** According to the Whim Privacy Policy, "We store information about your trips. This includes the start and end points of the trip, the start and end times of the trip, the method of travel, and the cost. This information is associated with your unique user identifier. This information is vital for the functioning of the service, as it allows us to provide the service and to ensure the trip provider is compensated for the trip (MaaS Global, 2018)."
  - Other trip and travel related data include favourite locations, which may be stored on a map, and calendar data, which is an optional setting that allows users to request additional reminders and plans.
  - ***Other data:*** Non-personal data, such as IP address, access time, browsing habits, and other metadata associated with use of the app, may also be collected. While generally non-identifiable, if linked with other data it may become identifiable, in which case it will be treated in accordance with the privacy policy

The amount of data collected through the Whim App and service, and the note regarding third party processors reflects the complexity of privacy considerations in MaaS applications. A stylised, high-level overview of a MaaS-style data ecosystem is presented in Figure 1.

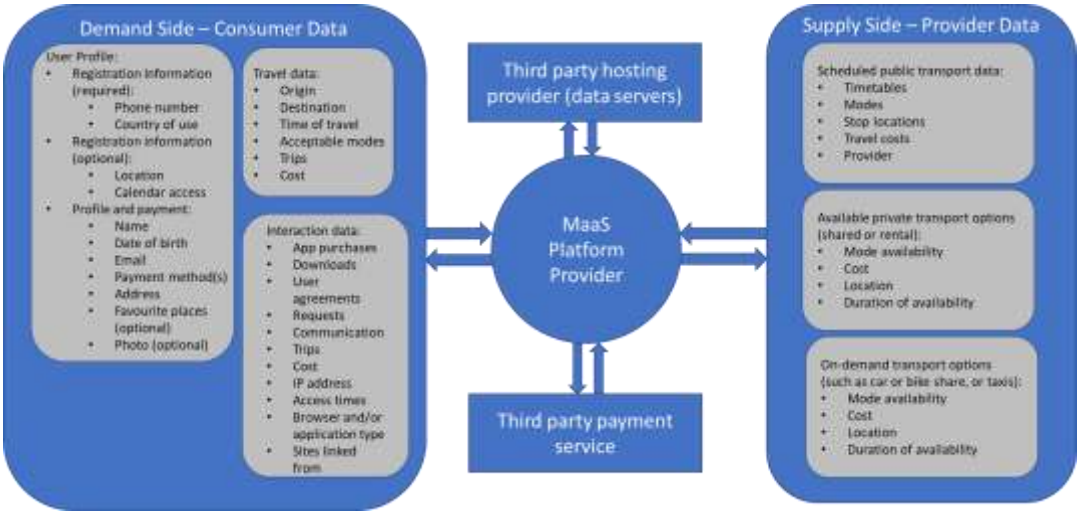

Figure 1: High-level conceptualisation of a MaaS-style data ecosystem (portions modified from König et al, 2016)

The Whim Privacy Policy, in addition to providing information on types of data collected, further provides information on the use of said data, and how it will be shared and treated with respect to third party interests, such as payment processors and hosting providers, which whom data will be shared. With respect to the latter, it is notable that they indicate the following: "As most other service providers, we store and process your personal data (if any) on third party servers (" Hosting Providers"). The Hosting Providers we have chosen enable us to keep your data in the European Economic Area (MaaS Global, 2018)." Such a territorial observation is notable, particularly when looked at in conjunction with the following statement (under "Disclosure of the Information to Third Parties"): "Our products and services may be provided using resources and servers located in various countries around the world. Therefore your personal data may be transferred across international borders outside the country where you use our services, including to countries outside the European Economic Area (EEA). In such cases we ensure that there is a legal basis for such a transfer and that adequate protection for your personal data is provided as required by applicable law... (MaaS Global, 2018)." Such a statement provides an implicit recognition of territorial requirements of the GDPR.

The privacy policy also indicates current approaches being taken for privacy and security, including the following:

- We use industry standard security mechanisms to protect the collected personal data. All collected personal data is stored in protected databases located behind a firewall and with both physical and software-based access controls provided by our Hosting Provider.
- Our payment providers are PCI-DSS Level 1 certified.
- We pseudonymise and encrypt the personal data;
- We have a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing (MaaS Global, 2018).

While useful in terms of indicating that the approach being taken is responsive to privacy considerations raised in MaaS applications, the degree to which it may be easily understood by the layperson is questionable – PCI-DSS Level 1 certified and pseudonymisation may not be concepts with which the general public are familiar, for example. However, information is provided regarding how to request that data are deleted or removed from the system.

The Whim Privacy Policy is a useful example for understanding how the GDPR may impact upon MaaS applications in the future. While it presents only surface information, without explicitly demonstrating the underlying technical and network considerations that allow for functionality, it does demonstrate how critical information may be usefully shared with users in more understandable language, as well as addressing some of the core concerns of the GDPR in terms of how it relates to location-based services. As a publicly-facing portion of the project, developing effective privacy policies that provide critical information to the user without overwhelming them with technical considerations will be an increasingly important element of app and system design, and should reflect 'privacy by design' principles in action.

Conclusion

Given rapidly evolving models of transport service provision, it is essential to ensure that their underlying data resources are managed in a way that is compliant with regulations, acceptable to consumers and responsive to provider needs in a competitive environment. Mobility as a Service environments represent complex networks of public and private service providers and users, with a multiplicity of data resources including open data (such as public transport schedules), commercially sensitive data (including fees and service availability), and personal user data (such as financial information and travel plans). In the context of such an ecosystem, consumer trust is a critical factor. The potential for individual travellers to be uniquely identified through their travel behaviours is significant, and ensuring adequate protection, and communicating this effectively, will be necessary to fully meet societal expectations.

To realise the potential offered by MaaS, then, it is necessary to ensure that the value-adding activities they enable, such as analysis of consumer needs and enrichment of data ecosystems, are supported by effective data management. The full benefits, however, can only be realized if these processes are driven by and managed in the context of agreed data protection policies and regulations to ensure that data producers continue to provide and share data with commercial entities. Such data management is becoming an increasingly complex and sensitive issue, with disparate data streams being sourced from multiple providers (including the individual traveller) and brought together for applications across the transport network, some of which were intended from the point of collection, but others of which opportunistically draw upon relevant populations and attributes to enhance the overall available information. The geographic scope of such applications is also increasingly complex, as MaaS services and their technology platforms may be spatially removed from the populations they serve.

As affected organisations continue to refine their approaches to General Data Protection Regulation compliance, it is evident that it will have serious implications for the potential development of Mobility as a Service applications. There is clearly a need for more targeted attention to be given to how technological and policy measures may be used to ensure compliance with the various emerging considerations and that users are confident that their data are being handled appropriately. Given the multiplicity of interests involved in MaaS provision, as indicated in the Whim case study, it will be critical to ensure that privacy issues and response to GDPR are raised early and that all involved parties are working with consistent and transferrable approaches that are accurately and clearly conveyed to the user. To do so will be beneficial not only to the service providers, who will avoid compliance issues and potential fines, but also to the users, who will be able to be confident that their data are being treated with adequate respect and protection.

References

1. Andrienko, G., Gkoulalas-Divanis, A., Gruteser, M., Kopp, C., Liebig, T., & Rechert, K. (2013). Report from Dagstuhl: the liberation of mobile location data and its implications for privacy research. ACM SIGMOBILE Mobile Computing and Communications Review, 17(2), 7-18.
2. Buckley, S., & Lightman, D. (2015). Ready or not, big data is coming to a city (transportation agency) near you. In Transportation Research Board 94th Annual Meeting (No. 15-5156).
3. Cavoukian, A. (2011). Privacy by design in law, policy and practice. A white paper for regulators, decision-makers and policy-makers.
4. Çolak, S., Alexander, L. P., Alvim, B. G., Mehndiratta, S. R., & González, M. C. (2015). Analyzing cell phone location data for urban travel: current methods, limitations, and opportunities. Transportation Research Record: Journal of the Transportation Research Board, (2526), 126-135.
5. Costantini, F. (2017). MaaS and GDPR: an overview. *arXiv preprint arXiv:1711.02950*.
6. Cottrill, C., Gault, P., Yeboah, G., Nelson, J.D., Anable, J. and Budd, T., 2017. Tweeting Transit: An examination of social media strategies for transport information management during a large event. Transportation Research Part C: Emerging Technologies, 77, pp.421-432.
7. Cottrill, C. D., & Derrible, S. (2015). Leveraging big data for the development of transport sustainability indicators. Journal of Urban Technology, 22(1), 45-64.
8. Cottrill, C., & Thakuriah, P. (2011). Protecting location privacy: Policy evaluation. *Transportation Research Record: Journal of the Transportation Research Board*, (2215), 67-74.
9. De Montjoye, Y. A., Hidalgo, C. A., Verleysen, M., & Blondel, V. D. (2013). Unique in the crowd: The privacy bounds of human mobility. Scientific reports, 3, 1376.
10. Department for Digital, Culture, Media and Sport (2017). Public Consultation: Security of Network and Information Systems.
11. Egelman, S. (2013, April). My profile is my password, verify me!: the privacy/convenience tradeoff of facebook connect. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 2369-2378). ACM.
12. EUGDPR.org (2017). GDPR Key Changes. Available online at http://www.eugdpr.org/key-changes.html. Accessed 6 November 2017.
13. Freudiger, J., Shokri, R., & Hubaux, J. P. (2011, February). Evaluating the Privacy Risk of Location-Based Services. In Financial Cryptography (Vol. 7035, pp. 31-46).
14. General Data Protection Regulation, 2016. 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, pp.1-88.
15. George, G., Haas, M. R., & Pentland, A. (2014). Big data and management. Academy of Management Journal, 57(2), 321-326.
16. Goşman, C., Cornea, T., Dobre, C., Mavromoustakis, C. X., & Mastorakis, G. (2016, April). Secure model to share data in intelligent transportation systems. In Electrotechnical Conference (MELECON), 2016 18th Mediterranean (pp. 1-8). IEEE.
17. Hashemi, M. (2017). The Infrastructure Behind Twitter: Scale. From the Twitter Blog, available online at https://blog.twitter.com/engineering/en_us/topics/infrastructure/2017/the-infrastructure-behind-twitter-scale.html. Accessed 3 January 2019.

18. Intelligent Transport (2018). 'MaaS app Whim heading to UK for the first time ahead of full roll out.' 29 March 2018. Available at https://www.intelligenttransport.com/transport-news/66471/maas-app-whim-uk-first-time/. Accessed on 20 July 2018.
19. Jagadish, H. V., Gehrke, J., Labrinidis, A., Papakonstantinou, Y., Patel, J. M., Ramakrishnan, R., & Shahabi, C. (2014). Big data and its technical challenges. Communications of the ACM, 57(7), 86-94.
20. Jittrapirom, P., Marchau, V., van der Heijden, R., & Meurs, H. (2018). Future implementation of Mobility as a Service (MaaS): Results of an international Delphi study. Travel Behaviour and Society.
21. Jittrapirom, P., Caiati, V., Feneri, A. M., Ebrahimigharehbaghi, S., González, M. J. A., & Narayan, J. (2017). Mobility as a Service: A Critical Review of Definitions, Assessments of Schemes, and Key Challenges. Urban Planning, 2(2), 13-25.
22. Kamargianni, M., Li, W., Matyas, M., & Schafer, A. (2016). A critical review of new mobility services for urban transport. Transportation Research Procedia, 14, 3294-3303.
23. Kamargianni, M., & Matyas, M. (2017). The business ecosystem of mobility-as-a-service. In Transportation Research Board (Vol. 96). Transportation Research Board.
24. Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. International Journal of Human-Computer Studies, 71(12), 1163-1173.
25. Kitchin, R. (2014). The real-time city? Big data and smart urbanism. GeoJournal, 79(1), 1-14.
26. König, D., Eckhardt, J., Aapaoja, A., Sochor, J. L., & Karlsson, M. (2016). Deliverable 3: Business and operator models for MaaS. MAASiFiE project funded by CEDR. Submitted to: CEDR Conference of European Directors of Roads.
27. MaaS Alliance (n.d.). What is MaaS? Available online at https://maas-alliance.eu/homepage/what-is-maas/. Accessed on 10 Nov 2017.
28. MaaS Global (N.D.). 'Mobility app Whim launches in West Midlands to make travelling easier for National Express customers.' Available online at http://maas.global/mobility-app-whim-launches-in-west-midlands-to-make-travelling-easier-for-national-express-customers/. Accessed on 20 July 2018.
29. MaaS Global (2018). Whim App Privacy Policy, Updated 24 May 2018. Available at https://whimapp.com/privacy/. Accessed on 20 July 2018.
30. Moovit (2018). Moovit Privacy Notice (en). Available online at https://moovitapp.com/en-us/legal/privacy-policy-en/. Accessed 4 January 2019.
31. Patire, A. D., Wright, M., Prodhomme, B., & Bayen, A. M. (2015). How much GPS data do we need?. Transportation Research Part C: Emerging Technologies, 58, 325-342.
32. Pigni, F., Piccoli, G., & Watson, R. (2016). Digital Data Streams: Creating value from the real-time flow of big data. California Management Review, 58(3), 5-25.
33. Svantesson, D., & Clarke, R. (2010). Privacy and consumer risks in cloud computing. Computer law & security review, 26(4), 391-397.
34. Wu, X., Zhu, X., Wu, G. Q., & Ding, W. (2014). Data mining with big data. IEEE transactions on knowledge and data engineering, 26(1), 97-107.
35. Zhao, F., Pereira, F. C., Ball, R., Kim, Y., Han, Y., Zegras, C., & Ben-Akiva, M. (2015). Exploratory analysis of a smartphone-based travel survey in Singapore. Transportation Research Record: Journal of the Transportation Research Board, 2(2494), 45-56.
36. Zheng, X., Chen, W., Wang, P., Shen, D., Chen, S., Wang, X., Zhang, Q. & Yang, L. (2016). Big data for social transportation. IEEE Transactions on Intelligent Transportation Systems, 17(3), 620-630.