UMIS Stakeholders' User Requirements' Report

Tope Omitola, Ben Waterson, Niko Tsakalakis, Richard Gomer, Sophie Stalla-Bourdillon, Tom Cherrett and Gary Wills

Executive Summary:

This report describes the result of the first work package, Task 1 (Elicitation of User Requirements), of the UMIS project. The UMIS project is a PETRAS-funded project that applies the techniques in engineering, computer science and law to research and develop a privacy-preserving and privacy-enhancing data governance framework and A.I. data protection models that can be deployed by data producers and third parties to facilitate legal and ethical usage of data in a Mobility-as-a-Service (MaaS) system. Our aim is that, by using our data governance framework and models, this will improve data privacy of the interactions of all the stakeholders in a MaaS system, including members of the public, thereby promoting mutual trust amongst these stakeholders.

The document starts by introducing the focus of our work, and goes on to describe Task 1 and its sub-tasks. It describes the rationale, methodology and the basis for our work. It goes on to describe our results, concluding with the next steps in the project.

Contents

1. INTRODUCTION:

This section describes the problem areas and gives background to the UMIS project.

1.1 MOBILITY AND MOBILITY-AS-A-SERVICE SYSTEM (MaaS) - OVERVIEW:

Mobility is fundamental to economic and social activities, with modern economies and lifestyles not being possible without extensive transportation systems. It also affords a range of societal and economic benefits, from access to services and employment to economic development and cultural exchange. In a mobility pattern, each movement has an origin, a potential set of intermediate locations, a destination and a nature which is linked with geographical attributes [***S1***].

But current transport systems suffer from a number of intractable problems, including congestion, emissions of greenhouse gases (GHGs) and local air pollutants, accidents, social isolation and inaccessibility of amenities and services [***S2***]. At the same time, urbanisation, a growing population, delayed car ownership, electrification, increasing connectivity, and automation are ushering in a new future in transportation, with disruptive ramifications for many stakeholders, especially operators and regulators, plus new service expectations by citizens. This transformation has enabled the evolution of Mobility-as-a-Service (MaaS) into a concept that promotes the integration of transport services to provide one-stop access through a common interface [***S3***]. MaaS capitalises on the Internet of Things (IoT) to provide access to seamless multimodal mobility to the end-user. It has the potential to provide an alternative to private car ownership and could contribute to reducing traffic congestion, the impact of climate change and improve access to mobility for aging populations.

For the mechanisms behind MaaS to work well, a substantial amount of data collection and data transfer is necessary. Transport operators generate and consume data about services offered and journeys made. Authorities often require data about transport services and networks, both to ensure compliance and to support future planning. For users to plan journeys, they need to provide their travel plans, and to make journeys, they will need to supply payment credentials. End-users also consume data from the system. Collaborative sharing and linking of safe, useful data between stakeholders under secure and rights-respecting conditions will be vital for building a trustworthy MaaS system. To achieve this objective, MaaS stakeholders must be convinced of the benefits of multi-party data sharing across the lifecycle of data generation and consumption, and be confident that security, privacy, and ethical behaviour are ensured.

Data is becoming an increasingly valuable commodity. Transport operators, as owners and users of data, seek to maximise the value of their own data and to access external data sets that can help them serve their communities and operate efficiently. For example, many transport operators seek to enhance the passenger experience through personalisation, and

in pursuit of this goal, new systems and technologies are being deployed which capture more data about the state of the network and their passengers than ever before. But, for these passengers, who are both data providers and consumers, limited awareness about data collection and sharing, combined with uncertainties around data trust models and data ownership, undermine their capability to negotiate their terms of data sharing, to develop trust in it and to perceive incentives for doing so.

The data and datasets generated and consumed in a typical Maas system can be classified into three broad categories: (1) *data pertaining to passengers*, e.g. passengers' personal data, (2) *data pertaining to the other stakeholders in the system*, e.g. transport service providers, and (3) (some elements of) *open data*. The following personal data was identified as useful in [***S4***] for providing timely and relevant information to passengers:

a) Journey Plans: Knowing where and when a passenger wants to travel is needed to alert them to delays/disruptions;
b) Name: Allows staff/messages to provide a more personal touch;
c) Location: Using a passenger's location enables services like nearest station information, available facilities (on train/at station), accessibility-aware station guidance, etc.;
d) Photo: Helps staff find and identify any passengers requiring assistance more quickly thus reducing passenger anxiety of being forgotten as well as cutting dwell-time at stations;
e) (Dis-)abilities and related information: Helps staff provide efficient and effective assistance;
f) Degree of familiarity and confidence with a particular journey/station. Data pertaining to the transportation system itself include route and schedule data, vehicles' location data, maintenance, staff and operations data, and companies' financial data.

Just as there is value in having the data, there can be value in sharing that data. Sharing data has the potential to create benefits for transport operators and passengers, as well as the local authorities. Sharing data can facilitate the following [***S5***]:

- Promote transparency and increase awareness of the transport operators and their engagement with their passengers.
- Spur innovation and support research that can help transport operators plan better service and operate more efficiently.
- Enable cost savings for transport operators by using outside resources for data processing and analysis.
- Generate revenue (e.g., through advertising).
- Support improved customer information.
- Support other community functions, such as informing local authorities, real estate developers, and law enforcement agencies.
- Facilitate multi-agency and multi-modal mobility solutions (as in a MaaS).

- Support benchmarking activities that help transport operators track and improve their performance.

Although there is value in having and in sharing data, there are attendant risks in data sharing. Some of these risks include [***S6***]:

- Privacy risks are present whenever data is personal data. Sometimes, the potential for a data set to be combined with other data sets increases this risk.
- Security risks can be present if data provides special insight into infrastructure and the locations of the people who use the services that could be used in a physical attack. Throughout the data management and sharing process, there is also risk of a cyberattack exposing private data.
- Risks of data misuse can be present whenever data is shared. Although transport operators seek to mitigate this risk through data documentation, some users may intentionally or unintentionally misinterpret data, drawing conclusions that are incorrect.
- Strategic risks are defined as the risk that sharing data could compromise the transport company's ability to serve its customers. This includes risks to its reputation reputational damage) and the risk that the information will be used against the transport company (e.g., by competitors).

Numerous studies indicate that people are either unaware of what private information they are exposing or they do not understand what information they are consenting to share (e.g. [***S7***]). Previous work in PETRAS, such as [***S8***], identified fostering user trust in IoT systems are still to be addressed and are very paramount. In addition, other issues, such as how data management and analytics are done in a decentralised system, such as MaaS, could affect user control and user trust of IoT. In many cases, apps may intentionally or unintentionally collect a wide array of sensitive and personal data, such as location history, email addresses, phone numbers, financial information, and usage history of the apps installed on passengers' phones. Privacy and security concerns are further complicated because new cyber-physical vulnerabilities exist on many different levels, such as through the app, API, the cloud, or hardware. These novel vulnerabilities challenge existing risk management frameworks [***S9***] and introduce new demands on existing legislation and regulations [***S10***]. [***S11***] showed that information transparency through privacy policies can increase user trust in an IoT-enabled MaaS. A way to improve this transparency is to ensure that these policies communicate clearly the risks of data processing and linkage of data subjects' supplied records.

As data subjects interact with the MaaS, they will generate "contextual footprints", also known as behavioural surplus [***S12***]. These contextual footprints, and their lineage, need to be made manifest for data subjects so that they can have better control on any future evolution of the data. The capture and provision of the provenance of these data, and manifesting these in the privacy policies, will be key to providing better user control of their data, increasing user trust in the MaaS.

1.2 MaaS APPLICATIONS - Related Work

MaaS has become popularised since its introduction in 2014 [***S13***], and has generated great activity for public and private transport and technology actors around the world. This section describes some MaaS applications that had been developed in the intervening years, and provides a background of previous in the domain.

[***S14***] describes some MaaS applications. These applications include:

1. Route planning:

Route planning applications are intended to assist the traveling public to navigate cities easily, quickly, and to determine an efficient route from a point of origin to the point of destination. Most of these applications allow the user to choose the best route depending on several factors including route length, grade, and speed.

Advanced applications provide commuters with real time arrival times, stop locations, and real time vehicle delays for major transport operators and station facility information (e.g., parking fare, lift, wheelchair access, toilets, etc.). These applications utilize the mobile device built-in GPS to provide riders with their current location and then suggest the nearest station and the time that the next couple of trains will be leaving the station. Further, the applications provide platform information allowing the user to know in advance the leaving and arriving platform for their selected train.

Examples: (a) Journey Pro Provide the best route using various combinations of available modes and real time journey planning around some major cities in the UK, (b) Trip Planner Help a traveller to organize everything needed for a trip.

2. Ridesharing/carpooling/vanpooling

Ridesharing contributes towards reducing emissions by reducing the number of vehicles on roadways, increases travel options, reduces parking demand, and, more importantly, reduces transportation costs to participants [***S15***]. Real time ridesharing has the potential to make a difference by offering a new mode of transportation that dynamically matches drivers and riders, and automatically distributes the cost reduction of the commute between them while reducing security and safety concerns. In essence, smart mobile applications for ridesharing match drivers and passengers with common origin and/or destination. Some applications allow real time ridesharing and therefore drivers may pick-up riders on the way to their destination. The applications require users to register to support matching, payment, and, for some, a background check. Further, some applications in addition to route matching, the applications use other factors like gender, non-smokers, social network, and user ratings. The rating features are then used to determine whether the rider and driver should be matched in the future or not.

3. Traffic safety

In general, applications in this category serve as a vehicle black box, voice-to-text, managing teenagers/inexperienced drivers, and reporting vehicle accidents. The applications that

serve as a vehicle's black box mostly save vehicle data such as speed, date, time, and location. In addition to this, the applications continuously video record driving and save the information.

These applications use collision sensors to register incidents whenever there is abrupt deceleration. In such events these applications automatically display emergency contacts saved by the user like family, police, and insurance agents.

In line with the black box applications, accident-reporting applications make it easier for the user to contact emergency personnel, document accident details, file a real time insurance claim, and obtain legal advice from a qualified attorney in the user's area.

4. Parking information

They make parking easier for people or agencies as they travel through a city or area. Statistics show that across the UK, it takes an average of 6 min and 45 s to find a suitable parking space.

Most parking applications provide users with information like real time data on parking availability, pay-by-phone options, and alerts the user on remaining meter times.

5. Travel information

Most of these applications show real time traffic information so that the travelling public can be aware of highway or public transport network's status. Most applications provide key traffic information including live updates on accidents as soon as they appear across the road network, ongoing and planned roadwork listed by road, region, and county, and real time average travel speed and travel time between major junctions. Moreover, some applications use built-in GPS to locate users, therefore providing targeted traffic information in real time. Some applications provide more detailed information about lane level updates such as which lane is blocked by an accident or construction activities. This real time travel information enables road users to make an early lane change to unblocked lanes or change a route. This information also allows motorists to choose travel routes based on current real time traffic information. Such real time traffic and roadway information are crucial for improving traffic operations. In the end this has the potential to overall reduce travel time, reduce traffic congestion, and reduce vehicle emissions.

Example: UK Bus Checker Show when buses arrive and destination for 300,000 bus stops in the mainland UK.

[***S16***] provides a broader picture of MaaS stakeholders. They describe the following stakeholders:

1. **The MaaS Provider**

Firstly, it is of crucial importance to define who could be the MaaS provider. Via our interviews we concluded that there are two prevalent options. The MaaS operator could

either be a public transport authority or a private firm. Both options have advantages and disadvantages.

In the case where the transport authority is the MaaS provider, it is easier to secure that all the public transport modes of the city will be offered via such a service. In addition, due to the fact that in most cities the public transport authority is the one responsible for authorising (or procuring) all the other transport operators (i.e. taxi, car-sharing etc.), it would be easier to secure their participation in the MaaS service. Furthermore, the public transport authorities are frequently also the transport regulators and as such it may take less time to regulate to enable the MaaS concept. However, public transport authorities may find it too difficult to diversify or extend their role and this transformation could take years. Similar to many other public authorities, transport authorities' bureaucracy may slow down the innovation penetration. In addition, the public transport authorities are not-for-profit organisations and probably do not have the incentives or they are constrained by law to develop MaaS services that could really advance the travel experience. Concepts such as those that were discussed in the section above (i.e. offering discounts at coffeehouses, or free movies downloads etc.) are probably too difficult to be included in the MaaS service design due to fair competition standards. Another disadvantage of the public authority acting as a MaaS provider is the fact that the concept of roaming (connectivity with other cities) is challenging to achieve; it is out of their scope to develop services that could be used to other cities as well.

In the second case, the MaaS provider is a private firm. It could be a firm that is established with the sole purpose of offering MaaS services or an existing firm that will either diversify or extend its current services. Under this option, it is expected that the MaaS market would be developed faster. Private firms are driven by profit maximisation and they put a lot of effort on developing unique intelligence and know-how and on designing services that offer advanced and personalised experiences. Another finding from our interviews with transport operators is that private transport operators such as car-sharing companies and on-demand modes would prefer to provide their services via a privately owned MaaS provider as they believe that it has more incentives to promote their services. In addition, it is easier for a private firm to offer roaming services as scaling-up is one of the most companies' goals. However, it is expected that it will take a lot of time for public transport services to join the MaaS schemes. One additional possibility is that the public transport authorities would be afraid of losing their reputation as the transport integrator and provider of the city.

2. Transport Operators

Transport operators are one of the main suppliers to the MaaS provider and are positioned in the core business ecosystem. Transport operators sell their capacity to MaaS operators and provide access to their data via secure APIs (Application Programming Interfaces). To fully enable the MaaS concept by offering the required data, transport operators should ideally have sensors on their fleet, and ticketing systems that accept smartphone reading. Other mobility related services, such as parking and toll operators or EV charging

infrastructure operators could also be included in the concept and in the MaaS service design.

The MaaS provider creates value for the transport operators in several ways. First of all, transport operators via the MaaS provider have the opportunity to access a wider market and increase their market share. In addition, the MaaS operator could optimize demand and supply by knowing in real time the demand and the capacity of transport operators. This would be especially valuable in peak hours when some of the transport operators run on full capacity and the MaaS provider could redirect their demand to other transport operators and avoid passenger dissatisfaction. As such, transport operators have the opportunity to grow their revenue from previously 'unreachable' customer markets and increase the level of satisfaction of their customers. The MaaS provider also creates potential for competition between engaged transport operators leading to improved levels of mobility services.

3. Data Providers

The data provider(s) is the other key supplier to the MaaS provider. As the MaaS concept relies heavily on interoperable data availability, the role of the data provider is of critical importance.

The data providers offer data and analytics capabilities to MaaS providers. They process the data of the transport operators and collect data from a range of other sources (i.e. customers' mobile phones, social media etc.). The multi-dimensional, ubiquitous data capture, with mobile devices and sensors about services, infrastructure and users that a MaaS provider needs, should be stored and retrieved in a fast, reliable and secure manner. The traditional technology architecture will not be able to accommodate such unprecedented levels of scale, speed and data variability. As such, advances in big data need to be exploited in order to provide the technological foundation for large scale data collection, storage and analysis. Concepts that employ cloud computing, such as the NoSQL database technology will need to be explored to facilitate the agile and real time data management requirements. Scalable data warehouses and large distributed file systems must be regulated by strict security and data policy requirements to ensure the latest encryptions tools and protocols are applied and followed.

The data providers process, repackage and make the data available in interoperable formats (by interoperability, we mean the ability of all devices, systems and infrastructure within a single MaaS scheme, as well as among the whole global MaaS ecosystem, to communicate information by being able to read, understand and translate each other's data). Data interoperability is of strategic importance to the MaaS model. In order to achieve interoperability, regional as well as national and international data standards and protocols need to be proposed on a central policy level and adopted by the transport operators. Another aspect to consider here, is the fact that the MaaS model could be fully enabled by data being openly available. This can be expedited by creating policies and standards that support secure open data and sources. The data that each MaaS provider will require depends on its service design. Additional value could be created by making some data available openly, as Open Data. Open Data has the potential to support innovative new

uses of data, for instance the incorporation of transport-related information into new services or apps. However, not all data is suitable for being published as Open Data, and personal data is one example of data that normally needs to remain closed in order to comply with data protection laws and to avoid creating risks to the data subjects [S32].

4. **Dynamic Multiservice Journey Planner Providers:**

There are numerous available journey planners in the market as well as open platforms for journey planning (i.e. OpenTripPlanner). The MaaS provider has the option to host an already available journey planner on its platform. However, the some of the currently available journey planners offer multimodal journey planning capabilities but barely any intermodal. In addition, they usually only include part of the available transport modes in an area focusing mainly on public transport modes (bus and underground), private vehicles, cycling and walking. Real-time information has started becoming a popular feature of the latest journey planners (wherever the appropriate data is available).

To enable the provision of advanced MaaS services, journey planners should develop new capabilities and especially intermodal planning capabilities that include all the available transport modes in an area (of course, this depends on the data that each transport operator provides as discussed above). In addition, journey planners should become dynamic; meaning to have the ability to adjust to a variety of anomalies (i.e. network disruptions, high capacity etc.) of the transport network and evaluate the most cost effective ways to get from A to B given the conditions on the network and the capacity of transport operators in real time.

The nature of the services that a MaaS operator envisages providing motivates journey planning firms and research communities to develop further innovation. The MaaS provider could add additional value to these firms by feeding them with data regarding users' location and demand.

5. **Ticketing and payment solutions providers:**

The technologies that are currently available regarding payment are quite advanced offering opportunities for payment with credit cards, smartphones and linking PayPal accounts. The MaaS provider could co-operate with firms that offer such capabilities so that the customers are able to pay for their MaaS purchases. Similarly, many technologies are available for ticketing with the most advanced one being digital wallets (smartphone wallets). Due to the fact that MaaS services are offered via smartphones, the ideal ticketing solution is these smartphone wallets. However, the technology a MaaS provider will choose depends heavily on the transport operators ticketing technologies. An ideal solution should be found so that the customer is able to access as many transport modes as possible with one ticket. Combinations of ticketing technologies could be another solution, but in this case the customer has to deal with holding more than one ticket. This would not be ideal as the core idea behind MaaS is to offer a simplified journey experience to users.

The MaaS provider generates extra revenues for both ticketing and payment solutions firms.

Technical backend providers and IT infrastructure: The MaaS model is enabled by technological breakthroughs such as big data availability and cloud computing. As such, it is of vital importance for a MaaS provider to co-operate with a reliable backend provider. Nowadays there are several on-demand cloud computing services that can respond to the needs of a MaaS provider. The MaaS model generates extra revenue to these providers.

ICT infrastructure: Internet connectivity is also critical to any MaaS provider. MaaS customers should be able to access the service via the MaaS mobile application or the website in real-time in order to request a transport mode for their journey. Furthermore, the MaaS operator should be able to transfer customers' requests and the data in real time. As such, high speed internet (3G and 4G) and widespread geographical internet coverage is a key enabler to the MaaS model. The MaaS model could further increase the revenue of the ICT companies

6. **Insurance companies:**

The MaaS model unravels new business opportunities for insurance companies providing them the option to expand their portfolio and increase their revenue. Traditionally, insurance companies' portfolios mainly focused on private motorised vehicles and their passengers' insurance, while in recent years they have been expanding in air-passengers' insurance and compensations (air passenger protection rights). In the MaaS market, there are several questions that insurance companies and legal offices will be called upon to provide solutions for. For example, what will happen in cases where the MaaS provider proposes a transport mode to a customer and the transport mode is unable to respond to the request in a given time window. The customer could claim passenger rights and request compensation. But the question is who is going to pay for this; the MaaS provider that proposed the mode or the transport operator that was not able to respond? Many similar questions will arise once the MaaS providers will start operating. This is a field that the research community could head to.

7. **Investors**

As mentioned above, preliminary estimations indicate that MaaS is a trillion dollar market providing an opportunity to investors to exploit. The MaaS market could attract not only private investors, but also public funds. For example, public authorities support concessionary travel schemes, while subsidize public transport operators, especially bus operators. Part of these funds could be redirected to MaaS providers as it is assumed that they could better match supply and demand saving as such public money and reducing bureaucracy. Another option is the crowdfunding. However, these options need further investigation on how could efficiently be applied.

8. **Regulators and Policy Makers**

Although, regulators and policy makers are positioned in the outer layer of the MaaS ecosystem, they are the key actors that could enable the MaaS market. Since this concept includes open data and open APIs, they are those that can provide and regulate for open

standards and interoperable data formats. For example, given the potential value of open and/or interoperable data within the MaaS ecosystem, regulators could play an important part in mandating openness and setting or encouraging adoption of technical standards. Regulators could also provide policy frameworks and recommendations for the sustainable development of the market, fair competition, financing, passenger rights, privacy and security, service quality standards, social inclusion, and safety. The ideal is the policy framework to be proposed by the government on a national level in order to avoid different open standards across different regions that will hinder interoperability. Moreover, as one of the goals of MaaS providers is to scale-up in several countries, the data interoperability standards could be proposed by an international organisation (for example, the MaaS Alliance is an NGO that has been established to promote this idea and enable the MaaS market). Regulators could spark the fire by providing these standards and then let the market grow. It is assumed that the development of the MaaS market would be similar to the telecommunication market (i.e. global standards for GSM networks – global roaming).

The MaaS model creates value to the society and to authorities. It provides opportunities for more efficient use of transport management tools and resources/data to meet the needs of citizens. It could also contribute to a more effective redistribution of the government's mobility subsidies. MaaS providers (in case of private firms) will pay taxes generating income for the governments.

Finally, the vision of the MaaS concept is to reduce car ownership while providing equally convenient but sustainable transport options. In doing so, this model contributes to sustainable development.

9. Unions / Lobby Groups

Unions usually slow the innovation penetration and could also slow the development of the MaaS market. A recent example is the one of Uber and the taxi unions; a private firm entered the on-demand transport market disrupting the business-as-usual model. This has resulted into legal fights, while in some cities Uber is not allowed to operate anymore. In order to avoid similar situations in the future, the authorities could develop checklists with the minimum standards a MaaS provider could have in order to operate in an area (licensing MaaS providers).

10. Universities and Research Institutes

Since MaaS is a new concept, research is needed in several sectors of the ecosystem as described above. Research could provide quantified evidence regarding all the aspects of this concept allowing the regulators to develop the appropriate enabling frameworks. Research could contribute to the technological innovation that is required to enable the MaaS idea. It could also assist with the development of the business models, the financing structures, the insurance schemes and the revenue allocation models. At this early stage, research is an important enabler of the concept.

11. Customers

MaaS is by definition a user-centric model. MaaS providers are established having as a vision to add value to customers and the society as a whole. Customers belong to the core business of the MaaS provider and are key players to the ecosystem. Based on the business model of the aaS provider (B2C, B2B, B2C&B2B) the customers could be individuals, companies or both. Another concept is that the MaaS providers could offer services not only to passengers, but also to freight sector. Further definitions are needed regarding who could be the customers of the MaaS providers. For the purposes of this paper, we consider passengers as the customers.

The MaaS model adds value to the customers by offering them hassle-free, price-worthy and personalised mobility. The demand for MaaS, the service design, the willingness to pay for using MaaS services and the impact that MaaS could have on travel patterns are topics that research is needed in order to motivate regulators to speed up establishing the standards. However, customer is the only actor that research has started conducting about. For example, [***S16***] proposed a framework to personalise MaaS services and mobility packages.

[***S17***] reports some MaaS examples in the EU and they further pointed out some of the core issues that need to be addressed before MaaS can be made palatable to different stakeholders. They observed that governance, not technology, is the key challenge for MaaS. System governance was a consistent topic in each city visited in the EU. While every region has a unique approach, all have faced and addressed questions of how to organize to implement MaaS and what institutional and regulatory frameworks are required. In order to encourage people to use MaaS, [***S17***] asked the following questions: What rules are required to govern mobility integration? How should urban data be treated to ensure both public usability and trust? How do we look at the regulatory environment more comprehensively—think about consequences on all fronts—and think holistically about setting policies while avoiding analysis paralysis?

They observed that MaaS systems will be based upon and will generate a continuous wealth of data. Private companies involved in MaaS are often data companies. They recommended that protocols are needed for open mobility data and use of APIs, so that harvested data can be used to right-size operations. In addition, data can also be used to allocate revenues in a MaaS system, and that rules are needed for privacy protections.

1.3 INTRODUCTION TO THE UMIS PROJECT

MaaS has the potential to benefit society, helping to solve many of the pressing challenges of modernity. In addition to the issues of data privacy risks, described above in Section 1.1, [***S13***] also noted that despite several trials with MaaS in Europe and a growing body of research on a variety of issues associated with MaaS, little attention has been paid, to date, to governance. Governance refers to what decisions must be made to ensure effective management and use of IT (decision domains) and who makes the decisions (locus of accountability for decision-making). Specifically, **data governance** refers to who holds the decision rights and is held accountable for an organization's decision-making about its data

assets [**S17B**]. **Data governance** is also related to building risk assessment into the data lifecycle, including security but also privacy and data protection risk assessment. Therefore, to foster user trust in MaaS systems, the governance underlying data sharing and inference needs to be addressed.

Our overall aim is to help ensure this establishment of trust in the use of MaaS by developing privacy-preserving data governance frameworks and A.I. data protection models that can be deployed by MaaS stakeholders (both data subjects and data controllers) to establish protocols for assessing risks when they make decisions about data sharing, as well as to facilitate legal and ethical usage of data, thereby promoting mutual trust. We have a four-pronged approach that helps us reach our goal. Our approach aims to: (i) reduce data movement as much as possible, (ii). reduce the number of data intermediaries in the ecosystem, (iii) build a governance structure, and (iv) ensure a high level of auditability for data access. By having Information Law at its core, UMIS takes a socio-technical approach to solving the privacy challenges in IoT systems. UMIS is co-created by user partners who will be using UMIS outputs in their work. UMIS consists of the following partners: The University of Southampton, Immuta, Solent Transport, and kn-i.

UMIS research questions are as follows: (a) How do we build in privacy in the data being produced and consumed by the different stakeholders in an IoT-enabled MaaS system? (b) How do we ensure that data management, inferencing and analytics performed by data controllers, data processors, and other third parties, do not diminish the privacy of data subjects? (c) How do we guarantee data subjects' control over how their data are shared? (d) How do our provided solutions of the aforementioned three questions increase data subjects' trust in the MaaS?

1.4 UMIS - METHODOLOGY OF WORK

The epistemology approach in this project is both empirical and pragmatic, in that we are looking for a practical solution to a real-world problem. How to share data between organizations, securely and still protect the rights of individuals.

The pragmatic approach also comes in the way we develop our scenarios. We have triangulated the development of our scenarios, we have used published scenarios in academic literature, detailed scenarios from our industrial partners (Solent Transport) and applications developed buy the other partners (Immuta and KnowNow) and along with applications from previous academic research projects.

We have structured the project into 4 tasks that feed into each other.

Task 1: Stakeholders' User Requirements Capture & Collation to establish data governance needs and requirements, using Solent Transport’s scenarios.

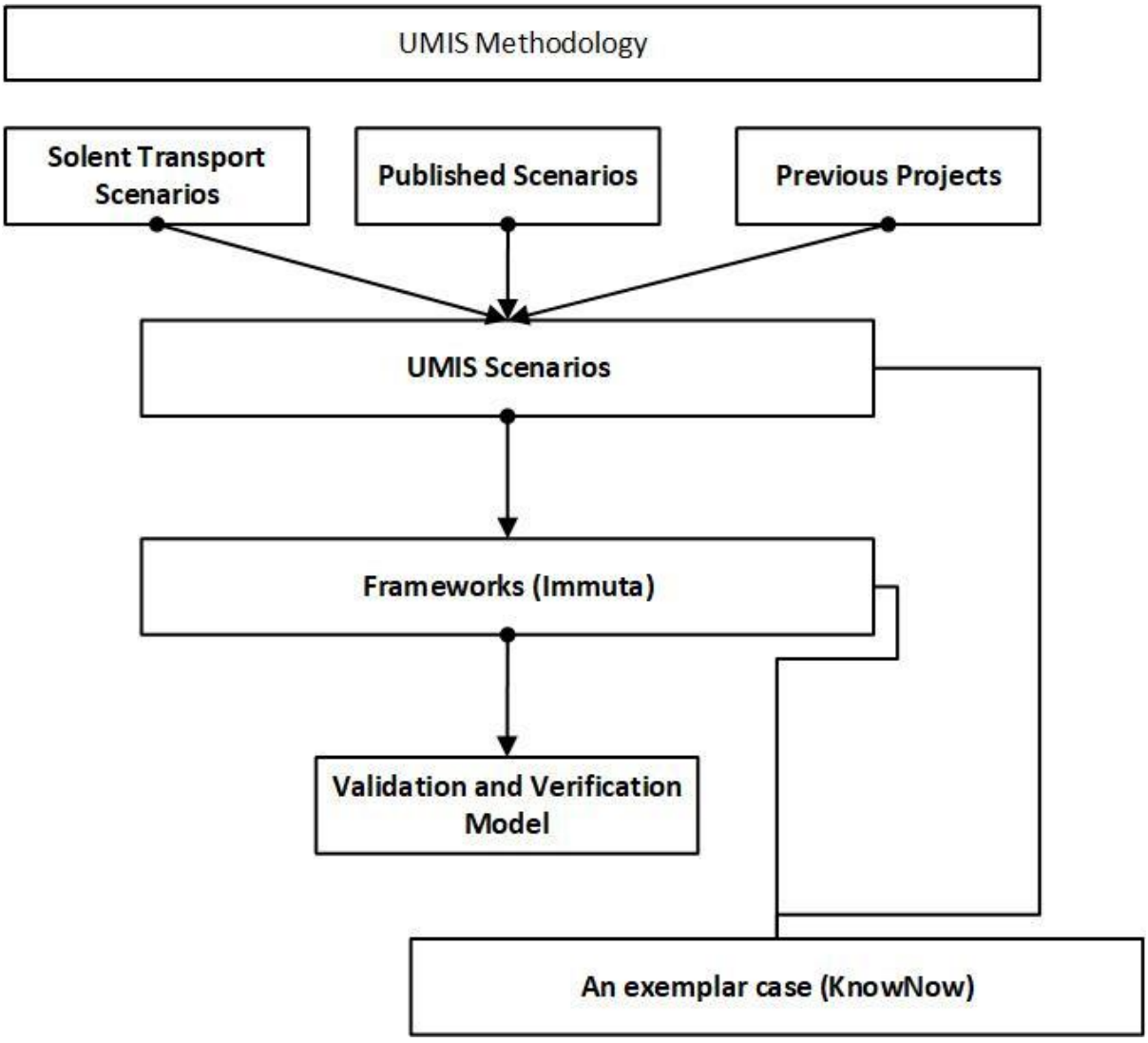
Task 2: Data Governance Framework, A privacy risk management framework, protocols and mechanisms, we will adapt the Immuta framework.

Task 3: Develop the Data Protection Model, to establish the appropriate 'soft' and 'hard' privacy-enhancing methods. We will use formal methods so we can explore the impact of any changes to the framework.

Task 4: Systems Integration, with Knownow, Consentua, a consent management platform that provides trustworthy customer journey and user experience.

While each is a separate deliverable in its own right, the impact comes with the synergy they bring. The aim is to provide our industrial partners and the academic community with

1. a framework to aid the government of data sharing building.
2. A model for which we can validate and verify any changes.
3. A set of mechanism that describe how to implement the policy
4. An exemplar system of the mechanisms working in an application.



2 TASK 1 – DESCRIPTION

This section lists the sub-tasks that comprise Task 1. These sub-tasks are:

2.1 User Centric Data Sharing Privacy Requirements

2.2 Scenarios and Use Cases

2.3 System Security Threat Analysis

2.4 Privacy Enhancing Data Ecosystem Requirements

2.1 TASK 1

In order to mitigate some of the privacy risks described above, in Section 1.1, especially in a MaaS system where different stakeholders interact and operate through different sets of relationships, it is important to determine the sources of threats and vulnerabilities in these interactions, and to assess the risks of these threats and vulnerabilities. **Risk** is a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence [***S18***]. A ***threat*** is any circumstance or event with the potential to adversely impact organisational operations and assets, individuals, other organisations, or through an information system via unauthorised access, destruction, disclosure, or modification of information, and/or denial of service. Threat events are caused by threat sources. A **threat source** is characterised as: (i) the intent and method targeted at the exploitation of a vulnerability; or (ii) a situation and method that may accidentally exploit a vulnerability. In general, types of threat sources include: (i) hostile cyber or physical attacks; (ii) human errors of omission or commission; (iii) structural failures of organisation-controlled resources (e.g., hardware, software, environmental controls); and (iv) natural and man-made disasters, accidents, and failures beyond the control of the organization.

2.1.1 USER CENTRIC DATA SHARING REQUIREMENTS ARCHITECTURE

User-centric data sharing requirements have their origin in concepts that existed since the 1970s,**[S19 – S20]** but were later expanded by the Information and Privacy Commissioner of Ontario Ann Cavoukian in her “Privacy-embedded laws of identity”. **[S21]** The main goal of the seven laws was to propose enhancements that put the user at the centre of data processing, offering greater control to the amount of data that will be processed and the way this would be done. At the same time, the laws recognised the need to supplement policy measures with technical designs that would architecturally effect privacy protections. **[S22]** Alongside these privacy principles, a discourse of ‘user-centric’ design and ‘privacy-enhancing technologies’ was created. **[S23]** Privacy-enhancing technologies and user-centricity were later endorsed by the European Commission **[S24],** and have eventually

found their way into the principles of 'data protection by design' and 'data protection by default' which are present in both the GDPR[1] and the UK's DPA 2018.[2] Data protection by design underlines all processing operations of personal data and calls for a careful consideration of the architecture, processing operations, possible risks and mitigating measures from the design phase and all throughout the lifecycle of the system. At the same time, data protection by default aims to maximise the user's control by ensuring that the maximum protection is the default setting and lowering it will be at the hands of the data subject.

In light of the above, UMIS is investigating the frameworks and data governance principles engendering user trust of how their data are shared in a MaaS. In UMIS, our stakeholders of focus include: (i) members of the public, i.e., passengers, (ii) transport operators, local authorities, data commissioners, 3rd parties, and other statutory bodies. These different stakeholders, in their different interactions in the MaaS, are users of the system. One of our aims is that these data governance principles enable frictionless data sharing, amongst the users, with minimal controls.

In the course of our investigations, we have developed a robust Data Sharing Requirements Architecture that can be used to inform and develop requirements for data platforms that will enhance user data privacy. In the UMIS Data Sharing Requirements Architecture, the data, metadata (data catalog and audit logs), query, and query results are parts of the sharing and access restrictions.

Level of Data Sharing and Access Restriction	**Direction of Movement of Generated Data**
Level 1: Strong Data Sharing and Access Restrictions	Data generated by an entity and the query results never leave this entity
Level 2: Medium Data Sharing and Access Restrictions	Data generated by an entity and the query results only leave this entity when an exception applies
Level 3: Weak Data Sharing and Access Restrictions	A copy of the data generated within an entity always stays accessible to this entity

Level 1. Strong Data Sharing and Access Restrictions: Here, the data, queries, and query results can only be shared and/or accessed within the entity in which it has been generated. In a multi-stakeholder environment, such as a MaaS, a super-governor, if available, can set common rules for all jurisdictions of the environment.

[1] GDPR article 25.
[2] UK GDPR article 25.

Level 2. Medium Data Sharing and Access Restrictions: Here, the data, query and query results can only be accessed within the entity in which it has been generated, but for specific purposes, data, query and query results can be accessed from other entities. An extension of this is when a super-governor is available, it can set policies for all the entities in all the jurisdictions.

Level 3. Weak Data Sharing and Access Restrictions: Here, a copy of the data, query or query results must sit within the jurisdiction in which the data has been collected. A further restriction of this type of access is that the copy sits within the entity in which it has been collected.

2.2 SCENARIOS AND USE CASES

In UMIS, we generated four scenarios of varying degrees of complexity of MaaS systems. These are:

1. A simple system, such as a taxi or private hire company, with (A) own fleet or (B) freelance drivers
2. An integrated ticketing train with bus journeys at each end
3. A larger scale system where the local authority coordinates (multi-mode, multi-operator) wide travel system, and where the local authority probably contracts a third party to operate the MaaS platform
4. A similar large-scale system, but here a private company (e.g. Stagecoach) coordinates (multi-mode, multi-operator) wide travel system, and where the local authority probably contracts a third party to operate the MaaS platform.

The next section will describe the different types and data interactions and flows in the aforementioned scenarios.

In this section, for each system of concern listed above, we will describe the stakeholders in the ecosystem, the data flows between these stakeholders, a table delineating the relationships between the stakeholders and the data interactions, and the applicable data sharing architecture pattern.

2.2.1 Scenario 1: A simple system, such as a taxi or private hire company, with its own fleet of drivers

This scenario is a simple interaction between passenger and a taxi company with its own fleet of drivers. This interaction may include other stakeholders that make the effective provision of the service possible.

The stakeholders here include:

1. Taxi company
2. Passengers
3. Metropolitan Authority / Council
4. The MaaS Commissioner, e.g., the taxi company

5. The Data Service Provider
6. Insurance companies and/or Tracking companies: These entities provide insurance services and tracking data for the taxi company, and
7. Employee Drivers of the company

Data Flows between the entities:

Figure 1 depicts, in graphical form, the data flows between the stakeholders.

1) Customer gives information to Taxi company (Name, where from/to, payment details)

    a) As this information is a contract between the customer and the taxi company, according to HMRC rules [***S25***] this data can be kept by the taxi company for a maximum of seven years

    B) The company has to ensure the information is secure (in transit and at rest).

2) Taxi then can use legitimate Interest as the reason to use this data for planning, efficiency, and fraud analysis, reputational damage, etc.

    a) It is allowed to use the data for analysis. However, it should only use the data it needs for processing. For example, there is no need to use personal data for planning.

    b) Care needs to be taken when sharing the results of the analysis that people cannot be identified. For example, an address is identifiable information.

3) Taxi companies can also pass on payment details to accountants.

    a) This is allowed as it is a subcontractor fulfilling a role.

    b) Care should be taken to pass on only the relevant details, for example, does the accountant need to know details of the journey or simply the name of the customer and payment details.

    c) Statutory retention period applies here.

4) The Taxi company can aggregate the data and pass it onto Metropolitan Authority/Council

Functionally anonymised data can be sent to public bodies, however, care needs to be taken to ensure that people cannot be identified in the data. Remember postcodes and addresses can be personal data, not just names. Also, relatively small number of journeys to an event or location could identify people (probation service, sexual health clinic, political party offices, etc.)

a. The public authority can hold this data under public task (public task - one of the lawful reasons that you can have to retain data).
b. As this does not contain any personal data there is no retention period.

c. Must be in the privacy notice
d. Data sharing agreement needs to be in place.
e. Security is still required even if thought to be Pseudo anonymised data

5) Taxi company to tracker/insurance. This is where information about the car miles travelled etc are recorded for maintenance, license, hire agreements etc.

a) Normally this has to be given as it is contractual. However, it should not contain the personal data of the passenger, nor the driver. The driver can be identified through a pseudonymised identifier.

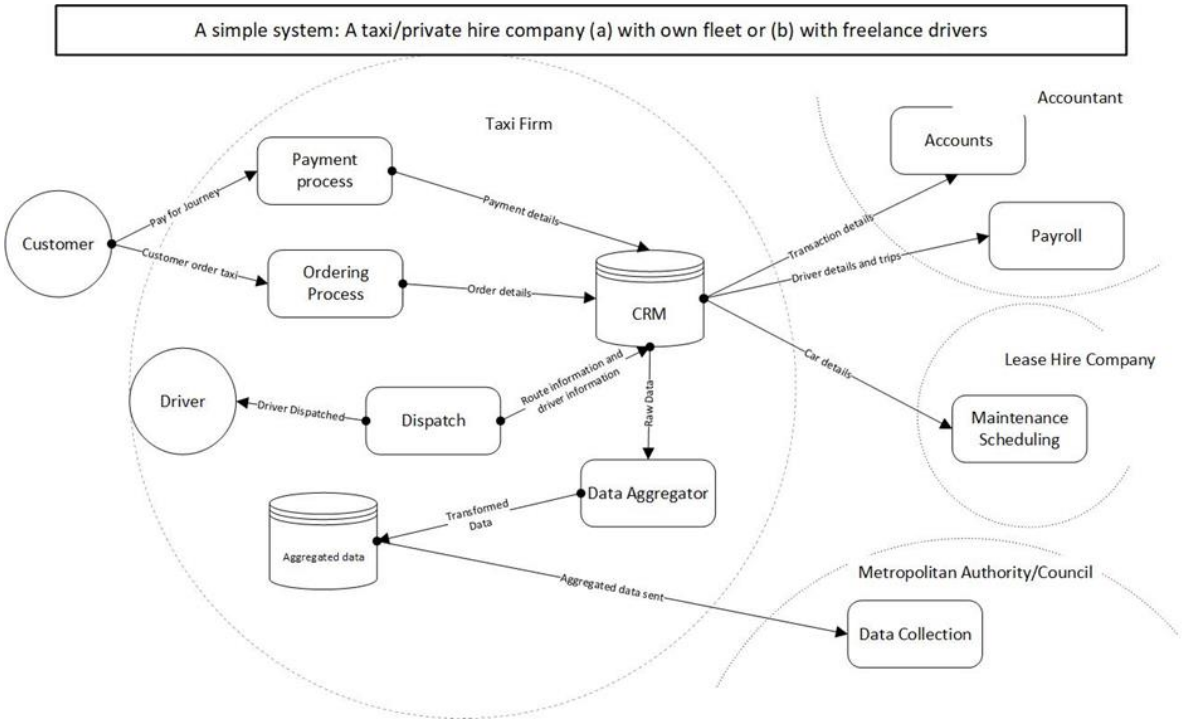


Figure 1 Depiction of data flows in a simple system involving a taxi company and other stakeholders.

Table 1 shows the entities that play the different roles and the type(s) of data they have access to.

Table 1 Roles and Entities and Data Access Types

Data governance role	Entity	Access to data/metadata
Data governor (set the policies to minimize the amount of data, de-identify)	Taxi company	Metadata

Data provider (makes the data available for consumption)	Passenger Taxi company Insurance companies/Tracking companies	Both data and metadata
Data user (consumes the data)	Taxi company Metropolitan Authority/Council Maas Commissioner Insurance companies	Both data and metadata Key question to answer: whether the data user needs access to individual level data or aggregates only

Applicable Data Sharing Architecture pattern.

In this scenario, Medium Data Sharing/Access Restrictions, i.e. Data generated by an entity & Query Results never leave this entity, suffice.

A passenger may grant access to his data including name, where from/to, payment details. The Taxi Company, the Metropolitan/Council and MaaS Commissioner have the permission to query this data. The Taxi Company can query it and access the full range of attributes at the individual level, depending on individual purposes. The Metropolitan/Council and Maas Commissioner can query it at the aggregate level. The Metropolitan/Council can also query derived aggregated data produced by the Taxi company. This can be queried by the Maas Commissioner. Data minimisation operations can also be carried out on the data.

Queries happen within the context of use cases or projects. Each project expires at a certain time. A data lineage tool would be useful to attach retention periods to derived data sources.

2.2.2 A simple system, such as a taxi or private hire company, with freelance drivers

This scenario is a simple interaction between passenger and a taxi company with freelance drivers. This interaction may include other stakeholders that make the effective provision of the service possible. Figure 2 depicts the flow of data between the entities

The **stakeholders** here include:

I. Taxi company
II. Passengers
III. Freelance Drivers
IV. Metropolitan Authorities / Councils
V. The MaaS Commissioner, e.g. Solent Transport
VI. Data Service Provider
VII. Insurance companies and/or Tracking companies

Data flow between the entities:

1. Customer gives information to Taxi company (Name, where from/to)

1. Company can keep this information for 7 years (HMRC rules [**S25**]) as it is a contract
2. This needed to be explained in the privacy notice.
3. The company has to ensure the information is secure (in transit and at rest).

2. Taxi can then use legitimate Interest as the reason to use this data for planning, efficiency, and fraud analysis., etc.

a. It is allowed to use the data for analysis. However, it should only use the data it needs for processing. For example, there is no need to use personal data for planning.
b. The retention period needs to be reasonable, i.e. one planning cycle, (say 3-5 years).
c. Company must complete a legitimate interest test.
d. This needs to be explain in the Privacy notice, we can check this
e. Care needs to be taken when sharing the results of the analysis that people cannot be identified. For example, an address is identifiable information.

3. Freelance driver can store customer payment details and CCTV of the trip

a. Customer passes on payment details to Freelance driver
b. This is allowed as it is a subcontractor fulfilling a role
c. Subject to HMRC rules
d. May use a third-party payment system such as WorldPay or Barclay's bank system for payments
e. CCTV regulations apply here
f. Must have their own Privacy Notice
g. Can pass information onto taxi company, but should be pseudonymised data

4. Taxi company can aggregate the data and pass it onto Metropolitan Authority/Council and Maas Commissioner

a. Functionally anonymised data can be sent to public bodies, however, care needs to be taken to ensure that people can not be identified in the data. Remember postcodes and addresses can be personal data, not just names. Also relative small number of journeys to an event or location could identify people (probation service, sexual health clinic, political party offices, etc)
b. The public authority can hold this data under public task (public task - one of the lawful reasons that you can have to retain data).
c. As this does not contain any personal data there is no retention period.
d. Again must be in the privacy notice
e. Data sharing agreement needs to be in place.
f. Security is still required even if data is thought to be pseudonymised or anonymised.

5. Freelance driver to tracker/insurance.

a. This is where information about the car miles travelled etc are recorded for maintenance, license, hire agreements etc., pseudonymised or data.

6. The MaaS Commissioner may want to set the sets rules for data sharing between all the actors involved. However, we have said that there is no Data Super-Governor actors here (more a case in the next scenario)

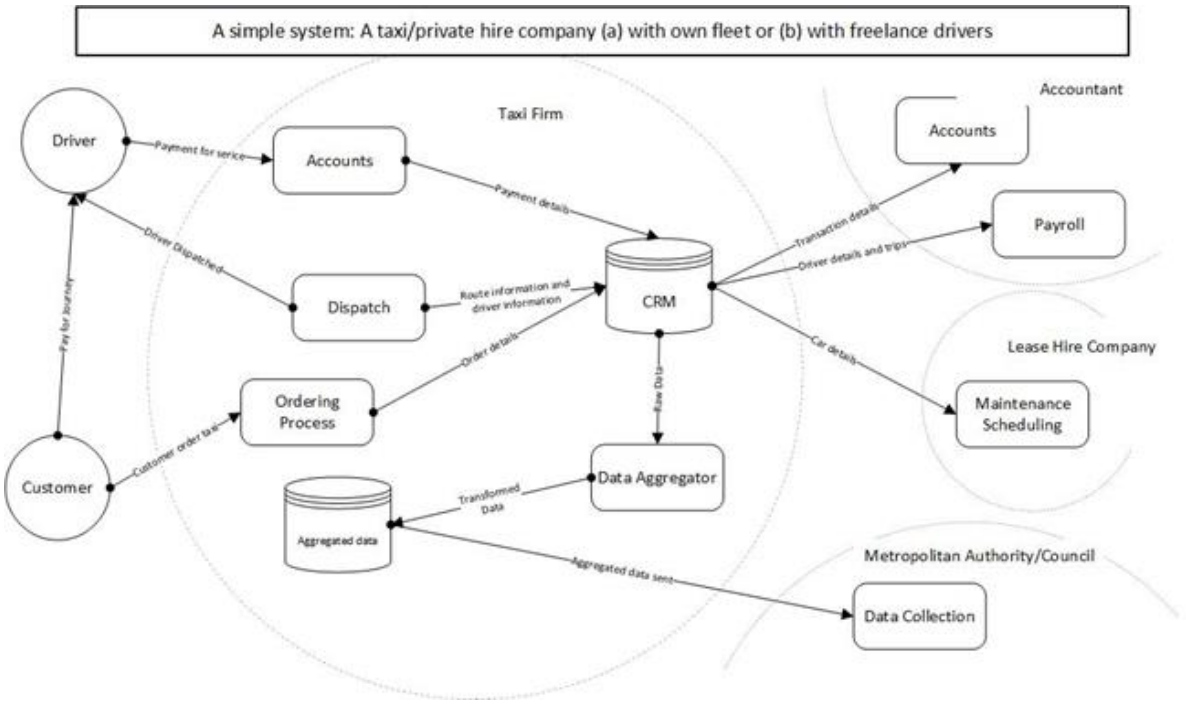


Figure 2: Data flow between the entities of a simple system of a taxi company interacting with the customer

Applicable Data Sharing Architecture pattern. The applicable data sharing architecture requirement pattern here is Medium Data Sharing/Access Restrictions, where data can only be accessed or shared within the entity in which it has been generated.

2.2.3 An integrated ticketing train service with bus journeys at each end

In this scenario, we have an integrated train service with bus journeys at each end, for example, a train journey between two cities with accompanying bus journeys. Figure 3 shows the data flow between the entities.
The **stakeholders** here include:

i. Train operator(s) and/or Tram operator(s)
ii. Bus operator(s) and/or Taxi companies
iii. Passengers, as they're data providers and trackable.
iv. Rail infrastructure companies, for example the companies involved with operating the ticket barriers
v. Metropolitan Authorities / Councils
vi. MaaS Commissioner (e.g., Solent Transport)
vii. The MaaS Provider. In this case, there could be more than one MaaS provider acting in different jurisdictions
viii. Data Service Provider
ix. Ticketing and payment solutions providers, for example, Trainline
x. Insurance companies and/or Tracking Companies

Data Flows between the entities:

1. Customer gives information to the Operating company (Account information, payment details, etc)
    a. Operator can keep the finance information for 7 years (HMRC rules) as it is a contract
    b. All other information can be kept for a reasonable time, can not be open ended.The retention period needs to be reasonable, i.e. one planning cycle, (say 3-5 years).
    c. This needed to be explained in the privacy notice.
    d. The operator has to ensure the information is secure (in transit and at rest)
    e. Operators then can use legitimate Interest as the reason to use this data for planning, efficiency, and fraud analysis., etc. Care needs to be taken when sharing the results of the analysis that people cannot be identified. For example, an address is identifiable information.
    f. Operators must complete a legitimate interest test for use of the daata beyond statutory/contractual or other legal obligations...
    g. It is allowed to use the data for analysis. However, it should only use the data it needs for processing. For example there is no need to use personal data for planning.
    h. CCTV regulations apply here
2. Operators can share the data
    a. Operators can share data with suppliers. For example payment details to accountants or the tracker company
    b. Care should be taken to pass on only the relevant details. Does the accountant need to know details of the journey or simply the name of the customer and payment details or the tracker company the name of the bus driver?
    c. Secure transfer personal data and security at rest is required.,
    d. Must be in the privacy notice that this is happening
    e. Data sharing agreement needs to be in place.
3. Operators and Aggregated Data
    a. Operators can aggregate the data and pass it onto Metropolitan Authority/Council, Maas Commissioner and infrastructure people.
    b. Functionally anonymised data can be sent to public bodies, however, care needs to be taken to ensure that people can not be identified in the data. Remember postcodes and addresses can be personal data, not just names. Also relatively small number of journeys to an event or location could identify people (probation service, sexual health clinic, political party offices, etc)
    c. Security is still required even if data is thought to be pseudonymised or functionally anonymised data
    d. Again, must be in the privacy notice
    e. Data sharing agreement needs to be in place.
4. The public authority can hold this data under public task (public task - one of the lawful reasons that you can have to retain data). As this does not contain any personal data, there is no retention period.

Table 2 shows the entities that play the different roles and the type(s) of data they have access to.

Applicable Data Sharing Architecture Requirements Pattern: The applicable data sharing architecture requirements pattern here is, Weak Data Sharing and Access Restrictions, where a copy of the data source is required to be situated within the entity in which it has been collected.

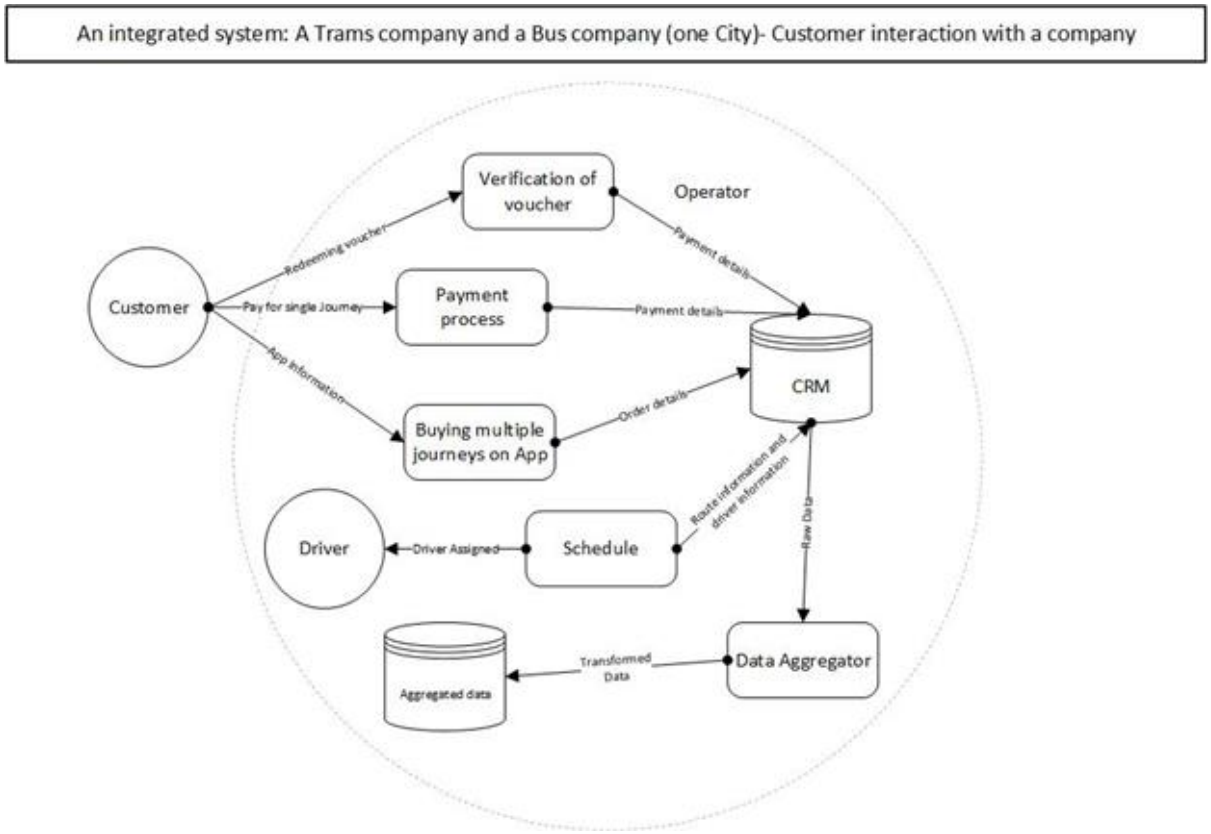


Figure 3 : Depiction of the flow of data between the entities of an integrated train service.

Table 2 Roles and Entities and Data Access Types

Data governance role	Entity	Access to data/metadata
Data governor (set the policies to minimize the amount of data, de-identify)	Maas Commissioner	Metadata

Data provider (makes the data available for consumption)	Passenger, Taxi company, Other transport companies, Rail infrastructure companies Maas provider Data Service Ticketing and payment Insurance company	Both data and metadata
Data user (consumes the data)	Taxi company Metropolitan Authority/Council Maas Commissioner Ticketing Insurance companies Data service provider	Both data and metadata

2.2.4 Large scale system, where the local authority coordinates area wide travel system.

This scenario focusses on a large-scale system where the local authority coordinates an area wide travel system

The **stakeholders** here, include:

i. Metropolitan Authorities / Councils
ii. Passengers
iii. Third party company
iv. Third party company's sub-contractors
v. The MaaS Providers, these could be the local council
vi. Data Service Provider(s), these could also be the local council
vii. Ticketing and payment solutions providers
viii. Insurance and/or Tracking companies
ix. MaaS Commissioner(s)
x. 3rd parties that need information but not directly involved, such as Department of Transport, the UK's Driver and Vehicle Licensing Agency, Commercial Suppliers providing IT infrastructures, such as IBM, Oracle, etc.

The different data controllers and processors are:

Data Controllers:

1. Train/Bus operators
2. Ticket operators

Data processors

1. Metropolitan Authority (more than one)
2. MaaS Commissioners

3. MaaS providers
4. Rail infrastructure
5. Data Services/IT infrastructure
6. Regulatory Authorities

Table 3 shows the entities that play different roles and the type(s) of data they have access to.

Table 3 Roles and Entities and Data Access Types

Data governance role	Entity	Access to data/metadata
Data governor (set the policies to minimize the amount of data, de-identify)	Maas Commissioner	Metadata
Data provider (makes the data available for consumption)	Passenger, Taxi company, Metropolitan Authority/Council Maas Provider Maas Commissioner Data service provider Insurance Company/Tracking company Third party companies and their sub-contractors	Both data and metadata
Data user (consumes the data)	Taxi company Metropolitan Authority/Council Maas Provider Maas Commissioner Data service provider Insurance Company/Tracking company Third party companies and their sub-contractors	Both data and metadata

Applicable Data Sharing Requirements Architecture patterns: Two main patterns are observed for this particular scenario, and they are:

1. Medium Data Sharing and Access Restrictions pattern of a “weak” Super Governor, where the super governor can set policies for all entities involved, but in a more flexible and weaker way

2. Strong Data Sharing and Access Restrictions pattern of a “strong” Super Governor, where the super governor is required, de-jure or de-facto, to set policies for all entities involved.

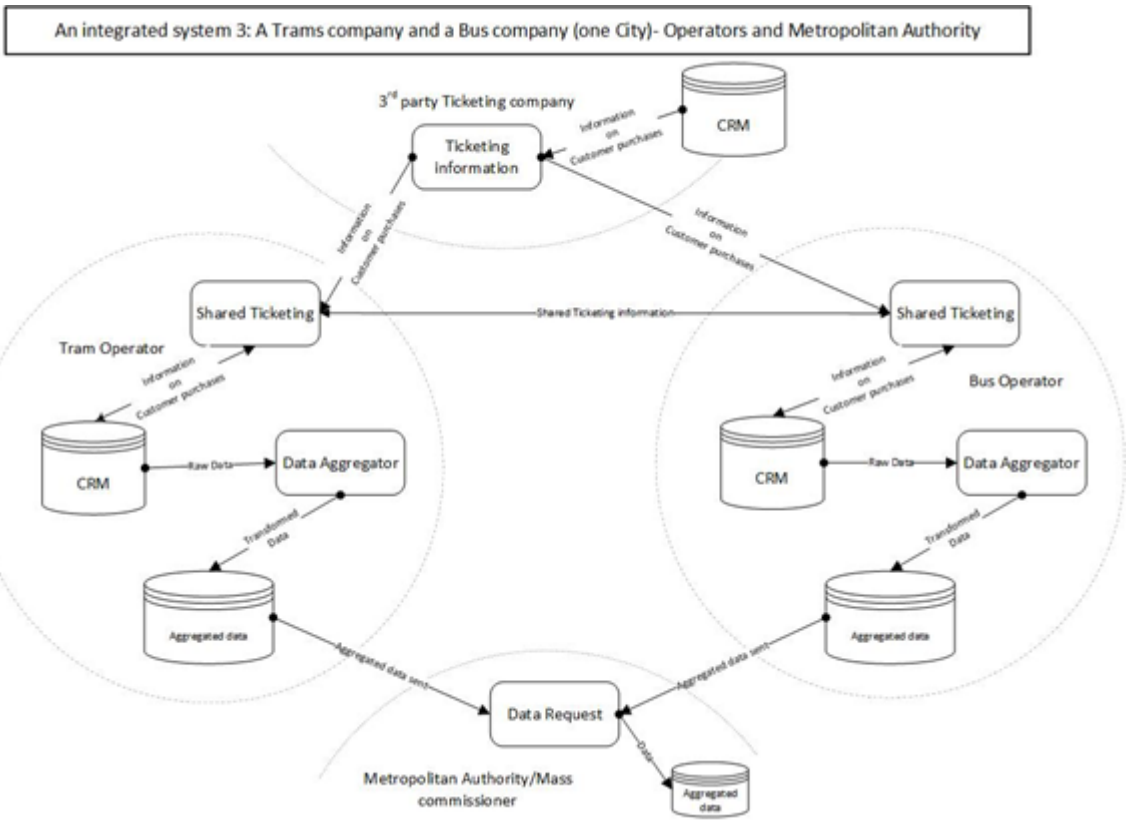


Figure 4 Data flow diagram for the integrated transport system. Showing the key data flows between the key entities.

2.2.5 A large scale system where a private company coordinates area wide travel system

This scenario focusses on the case where a private company, e.g., Stagecoach UK, coordinates the area wide travel system. Figure 6 shows the data flow between the entities in this scenario.

The **stakeholders** here include:

I. The Private Company
II. Passengers
III. Third parties
IV. Third parties’ sub-contractors
V. The MaaS Provider, this could be the private company
VI. Data Service Provider, this could also be the private company
VII. Ticketing and payment solutions providers
VIII. Insurance and/or Tracking companies
IX. Metropolitan Authorities / Councils

The data controllers and processors here are:

Data Controllers:

1. The private company as The Operator
2. Ticket operators

Data processors

1. Central Government (MaaS Commissioners)
2. Metropolitan Authorities (more than one)
3. MaaS providers (e.g., Stage Coach)
4. Infrastructure providers (e.g., Highway agency, National Rail, local authorities)
5. Data Services/IT infrastructure provider(s)
6. Regulatory Authorities (e.g., DVLA, Environmental Agency, UK's Information Commissioner Office)

Table 4 shows the entities that play different roles and the type(s) of data they have access to.

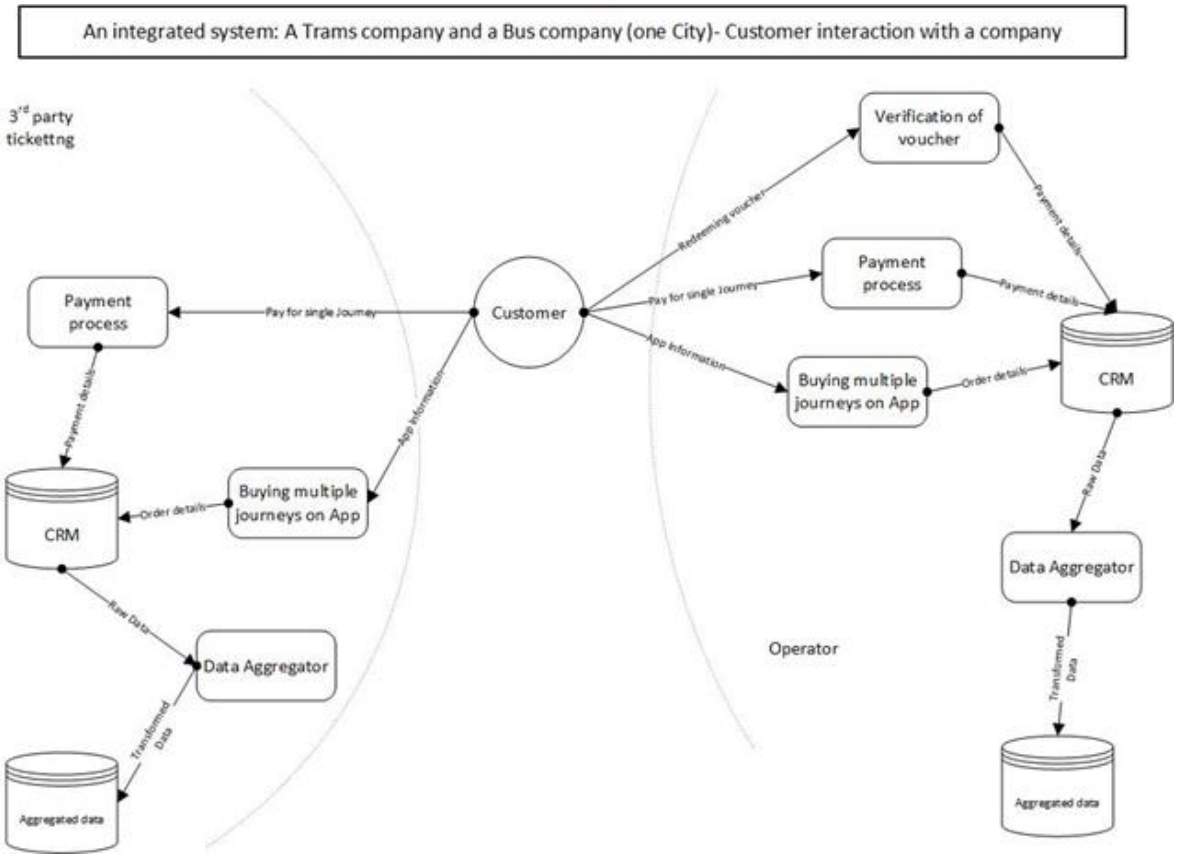


Figure 5 Data flow diagram for the integrated transport system. Showing the key data flows between the customer and the key entities.

Table 4 Roles and Entities and Data Access Types

Data governance role	Entity	Access to data/metadata
Data governor (set the policies to minimize the amount of data, de-identify)	Maas Commissioner	Metadata
Data provider (makes the data available for consumption)	Passenger, Taxi company, Freelance drivers	Both data and metadata
Data user (consumes the data)	Taxi company Metropolitan Authority/Council Maas Commissioner Data service provider Insurance Company/Tracking company	Both data and metadata

Applicable Data Sharing Requirements Pattern(s): The patterns here will be a mixture of: (i) Medium Data Sharing and Access Restrictions, where the data can only be accessed or shared within the entity in which it is generated or produced, with the addition of a "Super Governor" option that can set data sharing policies for all the other entities in the interactions; and (ii) Weak Data Sharing and Access Restrictions.

2.3 SYSTEM SECURITY THREAT ANALYSIS

In this section, we analyse the security threats that may ensue as a result of system operation. We have chosen one of the most complicated scenarios, a case of a large scale system where a private company coordinates area wide travel system. The system data flow of this scenario is shown in Figure 6, which we will use as the basis of our threat analyses.

We use the STRIDE methodology [***S26***] to the discern possible security and privacy threats.

Traditional security and privacy analysis methods, such as THROP [***S27***], work with threat

models that are based on the fault-error-failure chain model. While these models are valid to describe threats to single components, they are insufficient to describe system threats in complex interconnected systems, as we have in a MaaS and other IoT systems. OCTAVE [***S28***] is a risk based strategic assessment and planning technique for security, and mainly used to assess an organisation's information security needs. OCTAVE is best suited for enterprise information security risk assessments, which makes it unsuitable to analyse the security and privacy threats in a MaaS.

STRIDE, (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Escalation of Privilege), is a systems modelling tool that allows systems designers and analysts to develop an understanding of risks to a system and how to mitigate them. It helps designers to summarise the breadth of threats that a system may face, so that if the designer and analyst can understand where these threats may be realised in the system under design, they can create the systems solutions that can address these threats, thereby defending the system from attackers. By taking a threat-centric approach to security and privacy analysis associating each threat with a particular asset from attackers' perspective, STRIDE helps to change a designer's focus from the identification of specific attacks

to focussing on the end results of possible attacks.

Table 5, below, shows our application of STRIDE to discern possible threats to system operation

Table 5: Possible security threats to a MaaS system.

THREAT	PROPERTY VIOLATED
Spoofing The Customer	Customer Authentication
Spoofing the machines running the 3rd party ticketing processes	Authentication
Spoofing the 3rd party ticketing processes	Authentication; Authorization
Spoofing the machines running The Operator processes	Authentication
Spoofing the processes The Operator runs	Authentication ; Authorization
Spoofing the CRM DBs and other databases	Authentication ; Denial of Service
Tampering with the CRM Dbs	Integrity ; Denial of Service
Tampering with the network between The Customer and 3rd party ticketing company	Integrity ; Denial of Service ; Injection Attack
Tampering with the network between The Customer and The Operator	Integrity ; Denial of Service ; Injection Attack
Repudiation action of Customer that they paid for a journey while they have not	Non-repudiation of Customer actions
Repudiation action of 3rd party ticketing saying Customer has not paid while Customer has paid	Non-repudiation actions of 3rd party ticketing company
Repudiation action of Operator saying Customer has redeemed voucher while Customer has not	Non-repudiation actions of Operator
Repudiation action of Operator saying Customer has not paid while Customer has paid	Non-repudiation actions of Operator
Attacking logs of 3rd party ticketing company	Non-repudiation
Attacking logs of The Operator	Non-repudiation

Information Disclosure of the network between Customer and 3rd party ticketing, e.g. via Traffic Analysis or Eavesdropping	Confidentiality of transactions
Information Disclosure of the network between Customer and The Operator, e.g. via Traffic Analysis or Eavesdropping	Confidentiality of transactions
Information Disclosure against logs of 3rd party ticketing or The Operator	Confidentiality of customers' data and transactions
Information disclosure against Customer	Confidentiality of customers' data and transactions
Information disclosure against CRM Dbs	Confidentiality of customers' data; Confidentiality of companies' operations and financial data ; Confidentiality of Transport Infrastructure data
Information disclosure against 3rd party ticketing processes and The Operator processes	Confidentiality of companies' operations data
Denial of Service against 3rd party ticketing service	Availability of Ticketing service
Denial of Service against Operator service	Availability of Operator service
Denial of Service of network between Customer and 3rd party ticketing service, e.g. via message congestion of network	Availability of Ticketing service
Denial of Service of network between Customer and Operator service, e.g. via message congestion of network	Availability of Operator service
Elevation of Privilege against Customer, e.g., 3rd party ticketing or Operator sends corrupted data to Customer	Authorization
Elevation of Privilege through tampering with CRM Dbs	Authorization
Elevation of Privilege of Customer process inside 3rd party ticketing service or inside The Operator processes	Authorization

2.4 PRIVACY ENHANCING DATA ECOSYSTEM REQUIREMENTS

In this section, we describe the requirements that need to be ensured to enhance privacy in a MaaS ecosystem. These requirements include **privacy principles** as well as the **data protection principles**. We discuss how these principles apply to two of the major actors of a MaaS service, i.e., a taxi service provider (taxi company) and the MaaS App provider (App Provider). Finally, we describe the failure modes impacting these privacy principles.

2.4.1 Privacy principles

Starting from the GDPR and its data protection principles, the involved actors (i.e. the App Provider and the Taxi Company) must adhere to the data protection principles of Article 5. Note that the benefits of adherence are two-fold: the principles aim to provide guidelines against harm arising out of processing of personal data. At the same time, non-compliance in itself is penalised by the GDPR without an outcome that has led to material or immaterial harm. The data protection principles can be broken down into actionable obligations:

- **Lawfulness**

  - The Taxi Company is a data controller and, as such, it would have to operate under a predefined legal basis in order to justify the lawful processing of data. In the scenario of fulfilling a journey request, the legal basis may e.g. be the performance of a contract.
  - The App Provider, as a data controller, may be operating under performance of a contract (with the taxi company) or public task (if provider is an LA).

- **Fairness**

  - The Taxi Company will need to assess whether the models used, e.g., to calculate fares during peak hours – and their training data – are impartial resulting in no direct or indirect discrimination and define what the limitations of their models are.
  - Similarly the App Provider will need to assess whether the models behind the app (e.g. POI suggestions, taxi companies suggestions etc) have limitations or hidden assumptions.

- **Transparency**

  - The Taxi Company must ensure that its processing, the reasons behind it and the privacy measures are well explained and meaningful to its users, i.e. the passenger must understand which of their personal data are needed in order for the Taxi Company to be able to fulfil the requested journey.
  - The App Provider must also ensure that the information they provide to the user are meaningful to them, i.e. the user of the app must understand which information are requested for the functionality of the app and/or which information are passed on to

the Taxi Company to fulfil the requested journey (and any additional receivers/ purposes e.g. for planning).

- **Purpose limitation**

  - The taxi company will need to carefully scope the purposes for which data processing is allowed. In this example, the main purpose will be to fulfil a journey on behalf of the passenger. Additional purposes might exist, e.g. to pass on data to a financial institution for payment processing, data of the company's employees processed for the purposes of their employment etc.
  - The app provider must process the customer's data to facilitate the selection of the taxi company for the requested journey. Additional purposes might exist, e.g. for planning, for maintenance, for enhancement of features.

- **Data minimisation**

  - The taxi company will need to define the minimum amount of data to be able to fulfil the journey (see data assets in data flow breakdown)
  - The app provider will need to define the minimum amount of data to be able to hand off the customer to a taxi company, arguably a name, address, destination and journey status (if mapping functionalities exist). Special conditions might also exist, e.g. sensitive data such as medical conditions.

- **Accuracy**

  - The taxi company will need to establish tests to check the accuracy of the received data, since the majority of data will be passed on from the app provider, e.g. that the communication between the two is secure, that the data sent are the data received, that they arrive on time.
  - The app provider will need to establish test to ensure the data received are the data sent by the customer, e.g., that the communication channels are secure but also by form checks for correct format of emails, phone numbers etc.

- **Storage limitation**

  - The taxi company will have set up retention periods according to their processing purposes (performance of the contract) plus additional periods for e.g. non-repudiation or auditing or analytics of the communication with the app
  - The app provider will have set up retention period according to the purpose of facilitation, so minimum retention until journey is completed plus extra time for troubleshooting or auditing. Additional retention policies might exist for any additional purposes such as planning.

- **Integrity & Confidentiality**
    - Both will need checks in place to ensure that the data stored are the data received, that the data can be available when needed and that no unauthorised access to the data can be granted.
- **Accountability**
    - Both need active actions to demonstrate compliance, e.g. active monitoring and auditing.
- **Intervenability**
    - The taxi company shall have systems in place so that the customers can exercise their rights, e.g. a process to request the erasure of their data or the portability of their data to a different taxi provider.
    - The app provider shall also have systems in place for data subject rights, but the focus in this case will be on data stored by the data provider, e.g. user accounts or data for planning.

2.4.2 Data protection goals

The data protection principles outline a series of privacy requirements to guarantee legally compliant processing. The guarantee consists of sufficient technical and organisational measures to adequately reduce the "*risk to the rights and freedoms of natural persons*",[3] for example unauthorised processing. However, high-level data protection requirements to satisfy each principle exist throughout the Articles of the GDPR. To ease compliance efforts, the data protection requirements can be bundled into data protection goals [**S29**]. Data protection goals "*support the systematic implementation of legal requirements into technical and organisational measures and can therefore be regarded as 'optimisation requirements'*"[**S29, p.10**].

The data protection goals build on the protection objectives of information security by interpreting these objectives from the point of view of the data subject[4] and by adding data protection specific objectives. As a result, four goals are added on top of the security goals of Confidentiality, Integrity and Availability,[5] to form in total seven data protection goals:

1. Data minimisation, which aims to "*limit the processing of personal data to what is appropriate, substantial and necessary for the purpose.*" [**S29, p. 25**] The goal of data minimisation encompasses the GDPR's principles of data minimisation, storage limitation and data protection by default.
2. Confidentiality, relating to the GDPR's requirement by the same name but also requirements about data resilience and mitigation of data breaches. [**S29, p. 27**]

[3] GDPR recital 75.
[4] Since the aim shall be the protection against risks to the rights and freedoms of natural persons.
[5] The traditional 'CIA' model form the field of cyber security **[S20 – S31]**.

3. Integrity, referring to requirements for data to remain intact, complete, correct and up-to-date, but also continuously monitored and free from errors and discrimination. [**S29, p. 26**]
4. Availability, which includes requirements about the accessibility and retrievability of data as well as the restorability and resilience of data. [**S29, p. 26**]
5. Unlinkability, which implements the principle of purpose limitation and aims at ensuring that data shall not be linked. [**S29, p. 27**]
6. Transparency, which refers to transparency requirements for the data subjects as well as monitoring requirements for system operators and accountability and verifiability requirements to the supervisory bodies. [**S29, p. 27**]
7. Intervenability, which encompasses the requirement relating to the rights of individuals, i.e., the rectification, erasure and portability of data, the restriction of processing, the possible intervention in automated decisions, consent management and other measures to facilitate the exercise of data subject rights. [**S29, p. 28**]

The data protection goals, as classified by the Standard Data Protection Model, are accompanied by reference measures, both technical and organisational. However, the application of the measures that are appropriate in each case will be dependent on the particularities of the processing operation at hand. To assist in the selection of measures appropriate to satisfy each data protection goal, privacy assessments can consider the impact of failure modes.

2.4.3 Privacy Threats

A privacy threat further specifies the definition from section 2.1 as *any circumstance or event with the potential to adversely impact the privacy protection of an individual*, i.e. a threat will lead to a risk for the rights and freedoms of an individual. Privacy threats can identify what could cause a potential failure in meeting a data protection goal. Once privacy threats have been identified, they should be quantified in terms of likelihood and severity at a later stage. Privacy threats should not consider only whether a violation will result in harm. For example, failure to correctly perform data minimisation will result in sanctions even when it hasn't resulted in material or immaterial harm. Finally, all threats should be understood as ultimately impacting on the ability of the provider to provide the service.

Stage	Failure Mode	Point of failure	Principle	Goal	Threat
Service design	Relaxed/vague processing purpose	Taxi company	Purpose limitation Accountability Transparency	Data minimisation Transparency	Non-compliance; wrong legal basis; Overcollection of data
	Relaxed/vague processing purpose	App provider	Purpose limitation Accountability Transparency	Data minimisation Transparency	Non-compliance; wrong legal basis; Overcollection of data
	Wrong legal basis	Taxi company	Lawfulness	Transparency Intervenability	Non-compliance; unlawful data processing
	Wrong legal basis	App provider	Lawfulness	Transparency Intervenability	Non-compliance; unlawful data processing
	Wrong assumptions/limitations	Taxi company	Fairness	Transparency Intervenability	Inferences; discrimination
	Wrong assumptions/limitations	App provider	Fairness	Transparency Intervenability	Inferences; discrimination
	Inadequate documentation	Taxi company	Transparency	Transparency Intervenability	Non-compliance
	Inadequate documentation	App provider	Transparency	Transparency Intervenability	Non-compliance

Service provision	Irrelevant data	Taxi company	Data minimisation	Data minimisation Unlinkability	Overcollection of data; linkability; identifiability; detectability
	Irrelevant data	App provider	Data minimisation	Data minimisation Unlinkability	Overcollection of data; linkability; identifiability; detectability
	Inaccurate data	Taxi company	Accuracy	Integrity	Unlawful processing; unlawful retention; service delivery
	Inaccurate data	App provider	Accuracy	Integrity	Unlawful processing; unlawful retention; service delivery
	Corrupted data	Taxi company	Accuracy	Integrity	Unlawful processing; unlawful retention; service delivery
	Corrupted data	App provider	Accuracy	Integrity	Unlawful processing; unlawful retention; service delivery
	Altered data	Taxi company	Integrity	Integrity	Unauthorised alteration; inability to rectify data; inability to perform correct auditing; service delivery
	Altered data	App provider	Integrity	Integrity	Unauthorised alteration; inability to rectify data; inability to perform correct auditing; service delivery
	Unavailable data	Taxi company	Availability	Availability	Unlawful data collection; data minimisation; service delivery

	Unavailable data	App provider	Availability	Availability	Unlawful data collection; data minimisation; service delivery
	Unauthorised data	Taxi company	Confidentiality	Confidentiality Unlinkability	Unauthorised disclosure; identifiability; unauthorised processing
	Unauthorised data	App provider	Confidentiality	Confidentiality Unlinkability	Unauthorised disclosure; identifiability; unauthorised processing
	Inadequate documentation	Taxi company	Transparency Accountability	Transparency Intervenability	Limited information disclosure; failure to meet notification obligations; Unlawful processing
	Inadequate documentation	App provider	Transparency Accountability	Transparency Intervenability	Limited information disclosure; failure to meet notification obligations; Unlawful processing
	Insecure communications	Taxi company	Confidentiality Integrity	Confidentiality Integrity Unlinkability	Unauthorised disclosure; linkability; identifiability; detectability
	Insecure communications	App provider	Confidentiality Integrity	Confidentiality Integrity Unlinkability	Unauthorised disclosure; linkability; identifiability; detectability
	Inability to exercise data subject rights	Taxi company	Intervenability	Intervenability	Data accuracy; unlawful retention; unlawful processing;
	Inability to exercise data subject rights	App provider	Intervenability	Intervenability	Data accuracy; unlawful retention; unlawful processing;

3 NEXT STEPS AND CONCLUSION

As mobility is fundamental to economic and social activities affording a range of societal and economic benefits to a country's denizens, society needs to be cognisant of current transport systems in the provision of these mobility opportunities. The awareness that current transport systems suffer from a number of intractable problems, including congestion, emissions of greenhouse gases and local air pollutants, accidents, social isolation and inaccessibility of amenities and services is enabling the evolution of Mobility-as-a-Service (MaaS) to integrate transport services to provide an efficient one-stop access through a common interface. MaaS capitalises on IoT to provide access to seamless multimodal mobility to the end-user. It has the potential to provide an alternative to private car ownership and could contribute to reducing traffic congestion, the impact of climate change and improve access to mobility for aging populations.

As IoT technologies, such as MaaS systems, have evolved and become refined and effective, information collected and generated for one purpose may be, and are being, re-purposed for a different use, sometimes without the assent of the data provider. Many times, the data providers are members of the general public. This re-purposing of data could undermine the role assigned to individuals as acknowledged within current privacy and data protection laws, thereby adversely affecting the trust of members of the public. The aim of UMIS is to help improve the public's trust in the use of MaaS by applying the techniques in engineering, computer science and law to research and develop a privacy-preserving and privacy-enhancing data governance framework and A.I. data protection models that can be deployed by data producers and third parties to facilitate legal and ethical usage of data.

This document has provided the results of the first work package, Task 1, of the UMIS project, i.e., the gathering of requirements, and the rationale and methodology we used. Subsequent work will focus on the remaining tasks: Task 2 (The provision of the Data Governance Framework), Task 3 (Development of the Data Protection Model), and Task 4 (Systems Integration).

4 Appendix

In Section 2.2, we described the scenarios that we are focussing as exemplars in UMIS to discern some of the goals and purposes of our system-of-intent. This appendix first describes the methodology that we are using to more fully explore and describe the events that take place is these scenarios through a series of use cases that define the interactions between an actor and a system to achieve a goal. Use cases add value because they help explain how the system should behave and in the process of doing so, they help the system designer and analyst to elicit what may go wrong. This is then followed by a walkthrough-description of the use cases for Scenario 1 (A simple system, such as a taxi or private hire company, with its own fleet of drivers) to explore the perceived risks for the different actors.

4.1 1.1 Use Case Methodology

Use cases have become an integral part of modelling system requirements. A use case captures a contract between the stakeholders of a system about its behaviour. The use case describes the system's behaviour under various conditions as it responds to a request from one of the stakeholders, called the primary actor. The primary actor initiates an interaction with the system to accomplish some goal. The system responds, protecting the interests of all the stakeholders. Different sequences of behaviour, or scenarios, can unfold, depending on the particular requests made and conditions surrounding the requests. The use case collects together those different scenarios [**S29B**]. Use cases are fundamentally a text form, although they can be written using flow charts, sequence charts, Petri nets, or programming languages. Under normal circumstances, they serve to communicate from one person to another, often to people with no special training. Simple text is, therefore, usually the best choice.

The Use Case Writing Process involves the following:

1. Name the system scope and boundaries.
2. Brainstorm and list the primary actors.
3. Brainstorm and exhaustively list user goals for the system.
4. Capture stakeholders and interests, preconditions and guarantees.

   The system will ensure the preconditions and guarantee the interests.
5. Write the main success scenario.
6. Brainstorm and exhaustively list the extension conditions.

Include all that the system can detect and must handle.

7. Write the extension-handling steps.

8. Extract complex flows to sub use cases; merge trivial sub use cases.

9. Readjust the set: add, subtract, merge, as needed.

4.2 Example Use Cases (Scenario 1)

In the UMIS project, our scenario 1 represents a simple MaaS application (app) that allows a customer to book a trip, through the MaaS app, to a particular destination, using a private taxi firm. We assume the customer, i.e. passenger, had arrived in a city that they are not familiar with, and they know the location they want to be collected from and they know the location they want to go to. We also assume it is the first time they are interacting with the app.

Actors: Some of the actors involved with this scenario include:

(1) the traveller, (2) The MaaS app, (3) the taxi company, (4) the driver(s) of the taxi company, (5) Tracking companies, (6) Financial Services Provider

A successful journey in the scenario proceeds through up to ten use cases which can be grouped into four key phases :

1. Booking a journey

Use cases: request, availability, offer, payment, and conformation;

2. Starting the journey

   Use cases: approach, and arrival);
3. Journey in progress

   Use cases: monitoring;
4. Finishing the journey

Use cases: completion, and post-event

4.2.1 BOOKING A JOURNEY (REQUEST)

Actors:

The Traveller (primary), MaaS app

Events:

1. Traveller decides they want to go somewhere by taxi

2. Traveller opens the MaaS app (e.g. on mobile phone)

   2a. Traveller indicates a taxi journey is needed

3. Traveller requests specific journey and supplies information

3a. Required information: origin (start) and destination (end) locations

Note that the origin may not be traveller's current location

3b. Required information: desired journey time

Note that this may be either a specific start time, a required end time

(e.g. for airport arrival), or time bounds

3c. Additional information about the traveller(s): e.g., Wheelchair user,

unaccompanied minors, with pets, number of people, luggage, etc.

Data Needed or Supplied:

Journey Information & Traveller Information

4.2.2 BOOKING A JOURNEY (AVAILABILITY)

Actors:

MaaS app (primary), Taxi company

Events:

4. MaaS app passes Traveller & Journey information to a Taxi company

5. Taxi company decides whether they can service the request

   (e.g suitable driver and vehicle are available)

Note: This will require the Taxi company cross referencing the supplied Traveller and Journey information with their own internal data (vehicles, drivers, schedules, etc.) to determine if a suitable vehicle and driver is available for the requested journey and time. We assume here that this is either yes or no, not that an alternative variant is offered if the journey cannot be serviced exactly as requested.

6. Taxi company decides whether they want to service the request

   (Output: Yes or No)

7. (If 5 or 6 is no), Taxi company tells MaaS app NO

7a. App tells traveller NO

7b. Scenario ends, Data clean-up processes.

8. Taxi company tells MaaS app YES

8a. Taxi company sets a price and tells MaaS app

Data Needed or Supplied:

Traveller & Journey information

Service requests fulfilled or not

Financial quote for the journey

4.2.3 BOOKING A JOURNEY (OFFER)

Actors:

MaaS app (primary), Traveller

Events:

9. App offers price to traveller

10. Traveller decides to accept (yes) or reject (no) the price offer

11. (If 10 is no), Traveller tells MaaS app NO

11a. Scenario ends, Data clean-up processes.

12. Traveller tells MaaS app YES

Data Needed or Supplied:

Financial quote for the journey

Traveller's Decision to accept price or not

4.2.4 BOOKING A JOURNEY (PAYMENT)

Actors:

MaaS App (primary), Traveller, Financial Services Provider (FSP)

Note: We assume here for simplicity that the MaaS app is responsible for coordinating all financial transactions and that each journey is paid for individually. Alternatively, transactions could be handled more centrally (rather than within the front-end app itself)

between (a) the MaaS app provider and the Taxi company and (b) in the case of the traveller having a direct debit style account with the MaaS app between the MaaS app provider and the Traveller's bank. Such situations are considered in the other, more complex scenarios within the project.

Events:

13. App checks if it has traveller's financial details stored

14. (If 13 is yes) MaaS app confirms with traveller to use saved details

14a Traveller accepts (yes) or reject (no)

15. (If 13 or 14a is no) MaaS app requests card payment details

    15a. Traveller supplies card details (yes)

    or requests to pay on journey completion (no)

16. (If 14a or 15a is yes) App requests payment authorisation from FSP

16a. FSP provides authorisation (yes) or denies authorisation (no)

16b. (If 16a is yes) MaaS app takes money from FSP

16c. (If 16a is no) Scenario ends, Data clean-up processes

Data Needed or Supplied:

Traveller's Payment and FSP details

Corresponding (non-) Authorizations

4.2.5 BOOKING A JOURNEY (CONFIRMATION)

Actors:

MaaS app (primary), Taxi company, Financial Services Provider (FSP)

Events:

17. MaaS app tells Taxi company to service the request

17a. (If 16a is yes) then MaaS app uses stored financial information of taxi company to send payment

    (else) MaaS app informs Taxi company that journey is to be paid for

on completion

18. Taxi Company confirms booking to MaaS app

19. MaaS app confirms booking with traveller

19a. (if 16a is yes) MaaS app confirms payment complete

Data Needed or Supplied:

One or more journey identifiers and financial value

Journey Identifier & Decision (yes or no) if the journey is going ahead

Financial details of Taxi company

4.2.6 1.2.6 STARTING THE JOURNEY (APPROACH)

Actors:

Traveller (primary), MaaS app, Taxi company, Tracking company

Events:

20. Traveller opens MaaS app to check on estimated arrival time of taxi

20a. MaaS app confirms the journey identifier to be checked on

21. MaaS app requests vehicle identifier from the Taxi company

21a. Taxi company supplies vehicle identifier to MaaS app

22. MaaS app requests position data for vehicle from Tracking company

22a. Tracking company supplies vehicle position data

22b. MaaS app displays vehicle position to Traveller

Note: This event may be repeated multiple times either automatically or following a traveller manual request

Data Needed or Supplied:

One or more journey identifiers

Vehicle identifier

GPS vehicle positions

4.2.7 STARTING THE JOURNEY (ARRIVAL)

Actors:

Taxi Driver (primary), MaaS app, Traveller, Tracking company

Events:

23. Taxi driver arrives close to journey origin and notifies MaaS App.

23a. Taxi driver tells MaaS app vehicle and driver information
(e.g. name, profile photo)

24. MaaS app requests position data for vehicle from Tracking company

24a. Tracking company supplies vehicle position data

25. MaaS app provides taxi location and additional information
(e.g. number plate, vehicle colour, Taxi driver's name) to Traveller

26. Traveller physically locates Taxi

27. Taxi driver confirms traveller identity (e.g. using ID code in MaaS app)
27a Traveller confirms recorded destination is correct

28. (If 15a is no) Traveller confirms they will pay at journey completion

29. Journey starts

29a. Taxi Driver confirms to MaaS app that journey has begun

Data Needed or Supplied:

One or more journey identifiers

GPS vehicle position

Vehicle physical characteristics

Driver information

Traveller identification code

4.2.8 JOURNEY IN PROGRESS (MONITORING)

Actors:

Traveller (primary), MaaS app, Taxi Company, Tracking company

Note: While the steps in this use case are not essential for the journey to take place, it could be reasonably expected that a traveller could use the MaaS app to monitor a journey in progress, or alternatively that the Taxi company could monitor the journey in progress. This use case is therefore included here for consideration in risks.

Events:

30. Traveller uses MaaS app to check on current location and/or estimated arrival time

    30a. MaaS app requests position data for vehicle from Tracking company

30b. Tracking company supplies vehicle position data to MaaS app

30c. MaaS app displays vehicle position to Traveller

31. Taxi company tracks vehicle position

    31a. Taxi company requests position data for vehicle from Tracking company

30b. Tracking company supplies vehicle position data to Taxi company

Data Needed or Supplied:

GPS vehicle positions

4.2.9 FINISHING THE JOURNEY (COMPLETION)

Actors:

Taxi driver (primary), Traveller, MaaS app

Events:

32. Taxi arrives at destination

    32a. Taxi driver confirms journey complete to MaaS app

33. (if 15a is no) Taxi Driver requests payment

33a. Traveller pays Taxi Driver

Note: We assume here that this is paid in cash as if card payment was

required then details could have been supplied in 15.

33b. Taxi driver confirms payment received to MaaS app

33c. MaaS app confirms payment received to Traveller

Data Needed or Supplied:

One or more journey identifiers and financial value

4.2.10 FINISHING THE JOURNEY (POST-EVENT)

Actors:

MaaS app (primary), Traveller, Taxi Company

Events:

34. MaaS app asks traveller to rate Taxi service

34a. Traveller enters rating(s) on MaaS app

34b. MaaS app sends rating(s) to Taxi company

35. Scenario ends. Data clean-up processes.

Data Needed or Supplied:

One or more journey identifiers

Service rating

4.3 Summary of Risks

A recurrent theme in security analysis is that it is not sufficient to define good security and privacy controls solely within a particular abstraction or frame of reference: it is necessary also to consider what may happen if an adversary chooses to ignore that abstraction or frame. This arises, for example, in communication side channels, where an adversary may infer much from capturing radio frequency emissions from a cable, say, without needing to tap that cable physically. Similar eavesdropping effects have been observed against cryptography implemented on smartcards: simple analysis of the power consumption of the processor as it addresses each bit in turn can be sufficient to disclose the cryptographic key.

Although one may assume honest actors, the list of perceived risks below shows how some of these actors may deviate from the system's normal frame of reference.

4.3.1 COMMON OR SHARED RISKS

- The different actors' sharing financial data with others.
- Companies tracking of passengers
- Journey itinerary escaping from the system (insider or external threats)

User profiling either from individual journey data or from traveller's app usage

4.3.2 RISKS PERTAINING TO INDIVIDUAL ACTORS

Taxi Company / Driver

- Journey doesn't take place leading to wasted opportunity & time & costs
- Reputational damage [from e.g. rate your journey service]
- Client data escaping
- Journey details escaping [affects overall profitability, etc]

Financial Services Provider

- Reputational damage through client data escaping the system
- Forged cards or forged or wrong payment details being used

Tracking companies

- Reputational damage through client data escaping the system (e.g. journey details escaping the system and being illegally used by third party companies for unauthorised purposes)

MaaS App

[***From Traveller***]

- User accounts are not real people (fake accounts)
- Fake accounts making faking bookings using fake financial information leading to possible DoS attack

[From Taxi company]

- Reputational damage of selling services that do not arrive (or do not get serviced)
- Reputational damage due to client data escaping
- Impersonation of the app (by fake app providers)

[***From Tracking companies***]

- Reputational damage due to client data escaping

[***From Financial Service Providers***]

- Reputational damage due to client data escaping

5 REFERENCES

[S1] Rodrigue, Jean-Paul : The Geography of Transport Systems, pub. Routledge, 2020

[S2] SUstainable Mobility, policy Measures and Assessment, Final Publishable Report, 2005

[S3] Mukhtar-Landgren, D., Karlsson, I.C.M., Koglin, T., Kronsell, A., Lund, E., Sarasini, S., et al.,2016. Institutional conditions for integrated mobility services (IMS): Towards a framework for analysis

[S4] Treharne, Helen, Wesemeyer, Stephan, Schneider, Steve, Ross, Tracy, May, Andrew, Cockbill, Stuart, Akram, Raja N., Markantonakis, Konstantinos, Blainey, Simon, Pritchard, James and Casey, Matthew (2017) Personalised rail passenger experience and privacy

[S5] National Academies of Sciences, Engineering, and Medicine: Data Sharing Guidance for Public Transit Agencies – Now and in the Future. Washington, DC: The National Academies Press.https://doi.org/10.17226/25696, 2020

[S6] National Academies of Sciences, Engineering, and Medicine: Data Sharing Guidance for Public Transit Agencies – Now and in the Future. Washington, DC: The National Academies Press.https://doi.org/10.17226/25696, 2020

[S7] Miller, C. (2014, November 12). The Upshot - Americans Say They Want Privacy, but Act as if They Don’t, from The New York TImes: http://www.nytimes.com/2014/11/13/upshot/americans-say-they-want-privacy-but-act-as-if-they-dont.html

[S8] Maple, C, Susan Wakenshaw, Mariarosaria Taddeo: "Privacy and Trust Stream", Cybersecurity of the Internet of Things, PETRAS Stream Report, 2019

[S9] Nurse, J. R. C., Creese, S. and De Roure, D. 2017. Security Risk Assessment in Internet of Things Systems. IT Professional, 19(5), 20–6

[S10] Brass, I., Carr, M., Tanczer, L., Maple, C. and Blackstock, J. 2017. Unbundling the Emerging Cyber-Physical Risks in Connected and Autonomous Vehicles. Part I. In S. Appt

and N. Livesey (eds) See the Road Ahead. Connected and Autonomous Vehicles: The Emerging Legal Landscape (pp. 8–9). London: Pinsent Masons

[S11] Martin, K. D., Borah, A. and Palmatier, R. W. 2017. Data Privacy: Effects on Customer and Firm Performance. Journal of Marketing, 81(1), 36–58.

[S12] Zuboff, S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. 2019

[S13] Hensher, David & Ho, Chinh & Mulley, Corinne & Nelson, John & Smith, Göran & Wong, Yale. (2020). Understanding Mobility as a Service (MaaS): Past, Present and Future.

[S14] Siuhi, S, and J. Mwakalonge: Opportunities and challenges of smart mobile applications in transportation, Journal of Traffic and Transportation Engineering, Volume 3, Issue 6, December 2016

[S15] Dutzik, et. al. A New Way to Go the Transportation Apps and Vehicle-sharing Tools that Are Giving More Americans the Freedom to Drive Less; from [S14]

[S16] Kamargianni. M, and M. Matyas 2017. The Business Ecosystem of Mobility as a Service. 96th Transportation Research Board (TRB) Annual Meeting, Washington DC, 8-12, January 2017

[S17] American Public Transportation Association: Being Mobility-as-a-Service (MaaS) Ready APTA International Study Mission / June 2-8, 2019 Vienna, Hamburg, Helsinki , FINAL REPORT

[S17B] Khatri, V., and Brown, CV: Designing Data Governance, Communications of the ACM, January 2010, Vol. 53 No. 1

[S18] Geer, D., and R. Danzig: Mutual Dependence Demands Mutual Sharing, IEEE Computer and Reliability Societies 2017

[S19] Herbert Burkert, "Privacy-enhancing Technologies: Typology, Critique, Vision" in Philip E Agre and Marc Rotenberg (eds), Technology and Privacy (MIT Press 1997).

[S20] David L Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms" (1981) 24(2) Commun. ACM 84 doi: 10.1145/358549.358563.

[S21] Ann Cavoukian, 7 Laws of Identity the Case for Privacy-Embedded Laws of Identity in the Digital Age (White Paper, 2006) http://www.ontla.on.ca/library/repository/mon/15000/267376.pdf, accessed 11 June 2019.

[S22] Ann Cavoukian and Mark Dixon, Privacy and Security by Design: An Enterprise Architecture Approach (2013) https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-privacy-and-security-bydesign-oracle.pdf, accessed 20 January 2017, 7–14.

[S23] Lee A Bygrave, "Hardwiring Privacy" in Roger Brownsword, Eloise Scotford, and Karen Yeung, The Oxford Handbook of the Law and Regulation of Technology (Roger Brownsword, Eloise Scotford, and Karen Yeung eds, Oxford University Press 2017) 4–5.

[S24] European Commission, "On Promoting Data Protection by Privacy Enhancing Technologies (PETs)" (Communication) COM(2007) 228 final, 4.

[S25] HMRC: https://www.gov.uk/government/organisations/hm-revenue-customs (01.10.2021)

[S26] Potter, B: Microsoft SDL Threat Modelling Tool. In: Network Security 2009 vol. 1, pp. 15-18, 2009

[S27] Durrwang, J., Beckers, K., Kriesten, R.: A Lightweight Threat Analysis Approach Intertwining Safety and Security for the Automotive Domain. https://doi.org/10.1007/978-3-319-66266-4_20 2017 (01.10.2021)

[S28] Alberts, C., Behrens, S., Pethia, R., Wilson, W.: Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework, Version 1.0. CMU/SEI-99-TR-017. Software Engineering Institute, Carnegie Mellon University, 1999 at https://resources.sei.cmu.edu/asset_files/TechnicalReport/1999_005_001_16769.pdf (01.10.2021)

[S29] Conference of the Independent Data Protection Supervisory Authorities of the Federation and the Länder, The Standard Data Protection Model (v 20b, 17 April 2020).

[S29B] A. Cockburn: Writing Effective Use Cases, pub. Addison-Wesley, 2001

[S30] Matt Bishop, “Introduction to Computer Security” (Addison-Wesley Professional 2004).

[S31] International Organization for Standardization, Information technology – Security

[S32] Elena Simperl, Kieron O’hara and Richard Gomer, Open Data and Privacy, European Data Portal, https://data.europa.eu/sites/default/files/open_data_and_privacy_v1_final_clean.pdf