PETRAS

INTERNET OF THINGS
RESEARCH HUB

Increasing User trust in Mobility-as-a-Service IoT ecoSystem (UMIS) Project - Final Report

31 May 2023

Author(s): Tope Omitola, Ben Waterson, Niko Tsakalakis, Richard Gomer, Sophie Stalla-Bourdillon, Tom Cherrett and Gary Wills

Project/Stream title: UMIS / SRF2

TITLE OF REPORT

CONTENTS

List of Figures

List of Tables

TITLE OF REPORT

1. EXECUTIVE SUMMARY

The UMIS (Increasing User trust in Mobility-as-a-Service IoT ecoSystem) project investigated legal, scientific, and engineering techniques that can be used to encourage consumer trust and establish that trust in the usage of Mobility-as-a-Service (**MaaS**) system as part of the transportation provisioning ecosystem of a society. It was a joint project undertaken by the University of Southampton, Solent Transport, Immuta, and KnowNow Information (kn-I), combining the expertise from the domains of Law, Engineering, and Computer Science. UMIS sat within the Lens of "Law and Economics at the Edge" and within the "Transport and Mobility" Sectors of PETRAS.

MaaS is the integration of, and access to, different transport services (e.g., public ground transportation, vehicle-sharing, taxi, vehicle rental, etc.) on one single digital interface able to offer suitable solutions based on the user's travel needs. A MaaS interface should be available anytime offering integrated booking and payment as well as supporting service planning and improvement. These different transportation services are embedded in a MaaS ecosystem. MaaS ecosystems are Internet of Things (IoT) enabled complex networks of interconnected stakeholders within which a range of core transport services are integrated together to offer service recipients a set of options for each service request. These ecosystems exist in various configurations and can involve a wide range of stakeholders. A stakeholder is any entity involved in the processing of data generated within the ecosystem.

The list of potential stakeholders is varied, and may include: the MaaS provider, passengers of transport services, the Transport Authority regulating transport services, transport service providers, payment providers, ticketing providers, tracking providers monitoring the status of vehicles, stations, stops and luggage, and potentially cloud providers for data storage, computation, policy enforcement, mobile application providers, travel insurance providers, etc. In order to fulfil a service requirement, different stakeholders may need to interact together and exchange data. 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 ecosystem 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 assured during this lifecycle.

Numerous studies indicate that people are either unaware of what private information they expose, on the internet, or they do not understand what information they are consenting to share (e.g. [S1]), and previous work, such as [S2], identified fostering user trust in IoT systems as an area that is yet to be addressed. 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 [S3] and introduce new demands on existing legislation and regulations.

The aim of UMIS was to research and develop a privacy-preserving and privacy-enhancing data governance framework and data protection models that can be deployed by data producers and third parties to facilitate legal and ethical usage of data, thereby promoting mutual trust, between producers and consumers of data. UMIS research questions were 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? and (c) How do we guarantee data subjects' control over how their data are shared?

Our **methodology** involved the demarcation of the project into four tasks that fed into each other. These tasks were:

Task 1: The capture and collation of User Requirements, helping us establish data governance needs and requirements. We majorly used scenarios (both publicly available and scenarios developed by the UMIS teams)

Task 2: The investigation and development of a Data Governance Framework, which includes the research and development of a privacy risk management framework, with the corresponding protocols and mechanisms (taking advantage of the expertise of Immuta)

Task 3: The investigation and development of a Data Protection Model, which included the investigation of the security and privacy threats to MaaS, with the application of the Data Governance Framework (from Task 2) helping us develop the appropriate security and privacy properties of MaaS ecosystems, and

Task 4: The Systems Integration task with Consentua, a KnowNow provided consent management platform.

The project commenced during Covid-19 pandemic, and a major part of the work was carried on during the Covid-19 lockdown. Meetings were conducted remotely, every week with all the team members apart from Solent Transport. There were many highlights and lowlights of the project. One of the lowlights involved the inability of Solent Transport to provide us with (anonymised) datasets of customer journeys. Because of this, it was difficult to find out the effectiveness of our models on realistic datasets.

There were many highlights and insights. Some of the highlights included, inter-alia: (1) the setting out of the privacy and security threats in MaaS, (2) the security and privacy properties that a MaaS ecosystem needs to assure to establish trust within its data producers and consumers, as well as (3) the development of a Data Governance Framework that is privacy-preserving. Some of our major events on the project included the presentations of some of our results in reputable research publications, such as the 7th Conference on Internet of Things, Big Data and Security (IoTBDS) and the 30th ACM Conference on User Modeling, Adaptation and Personalization (UMAP), and also at most of the PETRAS internal events. Some of our insights included: (1) through applying Activity Theory [S4], we gained insight into delineating a complex ecosystem, such as a MaaS, into four layers of, Task, Primary Service, Operating, and Maintenance Layers and (2) by applying a "speculative design" approach to re-imagine legal interpretations of data protection principles within a MaaS use case, we gained insight into a fresh understanding and definition of the legal challenges in a typically data intensive IoT environment.

UMIS' main findings included:

1. The generation of use cases and scenarios of varying degrees of complexity in MaaS systems; these were:
   - A simple system, such as a taxi or private hire company, with (A) own fleet or (B) freelance drivers
   - An integrated ticketing train with bus journeys at each end
   - 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
   - A similar large-scale system, but here a private company coordinates (multi-mode, multi-operator) wide travel system, and where the local authority probably contracts a third party to operate the MaaS platform
2. The investigation and publication of the Data Governance Model, that can be taken up by data producers of a MaaS ecosystem and applied to their workflows, leading to increase of consumers' trust in the usage of MaaS
3. The investigation, development, and the publication of the pertinent security and privacy requirements of MaaS
4. The demarcation of a complex IoT system, such as MaaS, into a four-layer model of Task, Primary Service, Operation, and Maintenance Layers, and
5. The application of the four stages of design thinking, viz, Discovering, Defining, Ideating, and Assessing to defining the legal challenges of an IoT environment, and using this to propose an architectural design response to critique the notions of legal basis and necessity of a range of data production, inferencing and analytics.

UMIS' main findings helped us deliver on our research questions in the following ways:

I. The development of the user scenarios helped us capture salient User Requirements, which were deployed in our understanding of pertinent security and privacy threats in a MaaS ecosystem
II. This understanding helped in the investigation and development of the Data Governance Model, which
III. Was useful to develop the security and privacy properties (i.e. the Data Protection Model) to be ensured by data producers and consumers within MaaS ecosystems, while
IV. The Data Governance Model and Data Protection Model, applied by stakeholders within their workflows, will help ensure that data management, inferencing and analytics performed by data controllers, data processors, and other third parties, will not diminish the privacy of data of MaaS users, and thus
V. Helping individual members of the general public using MaaS to control how data about them are shared within that ecosystem.

2. SUMMARY DESCRIPTIONS OF PROJECT CONTEXT AND OBJECTIVES

2.1 UMIS' Background, Motivation, and Long-Term Vision

MaaS ecosystems are IoT-enabled, and as IoT technologies have evolved and become refined and effective, end-users continue to delegate important tasks to these technologies. When it comes to privacy of the generated data from ecosystem participants, the current forms of IoT technologies, such as an IoT-enabled MaaS system, have changed the nature of the problem. An IoT system may take information collected and generated for one purpose and re-purpose the same data for a different use, i.e. the data moves from primary to secondary uses. From the perspective of a MaaS stakeholder, such as a transport operator or an app provider, this makes the collected data much more valuable over time. In addition to re-purposing the collected data, these data can be commingled with other (possibly different) datasets, for vastly different purposes, further increasing the value of these datasets. With the re-purposing of datasets from their primary usage to secondary uses, the value of information in these datasets has moved from the primary purpose of why the data was collected to secondary usages. This re-purposing of datasets could undermine the central role assigned to individuals as acknowledged within current privacy and data protection laws. The concept of "notice and consent" underlying data subject intervenability for data collected at a particular point in time for particular purposes may be difficult to adapt for this current environment where innovative secondary uses have not been imagined yet. In addition, the opaque data cycles of an IoT-enabled MaaS environment result in a lack of transparency and traceability of data flows that are not necessarily compliant with data protection-by-design requirements and impinge on the data subjects' ability, especially passengers, to make informed decisions about their collected information. This inability to make informed decisions leads to erosion of trust in data subjects while interacting with the MaaS system. Successful deployments and operation of next generation transport systems will require mechanisms for establishing and maintaining trust in the systems' ability to provide clarity of data ownership and data sharing practices between data controllers, processors and other third parties in the ecosystem. One of the questions then becomes how do we balance users' control over their data versus users' trust in their interactions with the other stakeholders.

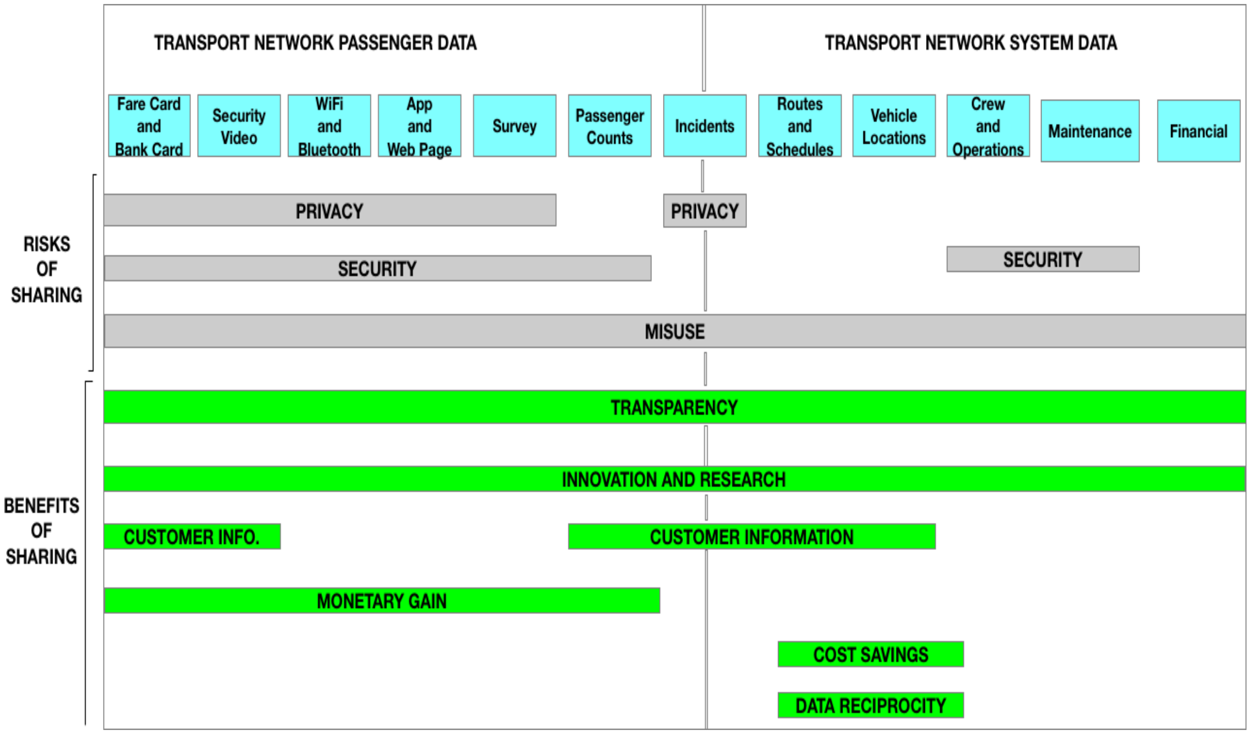

Figure 1 - A Mobility-as-a-Service System and its data types

Figure 1 shows typical MaaS data types and sharing characteristics. The following personal data was identified as useful in [S5] 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.

As Figure 1 shows, there are benefits to data sharing in a typical MaaS. These benefits include: (a) Cost Savings to passengers and transport operators; (2) Transparencies of fare costs, useful for passengers; (3) Savings for both passengers and transport operators. There are also attendant risks. These risks include: (1) Intentional and Accidental Misuse of Data; (2) Security risks against passengers and the transport operators; (3) Data Privacy.

Therefore, to foster user trust, in the privacy of their data, in MaaS systems, the governance underlying data sharing and inference needs to be addressed. UMIS' aim was to help ensure this establishment of trust in the use of MaaS by applying techniques in engineering, computer science and law to research and develop a privacy-preserving and privacy-enhancing data governance framework and data protection models that can be deployed by data producers and third parties to facilitate legal and ethical usage of data, thereby promoting mutual trust.

One of UMIS' long term visions is that a scalable Data Governance Model, such as ours, can be deployed by a data producer in a MaaS ecosystem, applied to their workflow, and shown to ensure the non-diminution of data privacy of MaaS systems' users.

2.2 Research Objectives and Corresponding Deliverables

Table 1 shows UMIS' research objectives and their corresponding deliverables.

Table 1 - UMIS' research objectives and their corresponding deliverables

Research Objective	**Deliverable**
Capture and Collate User Requirements	Work Package (WP) 1: UMIS Stakeholders User Requirements Report
Investigate and Develop Data Governance Framework	WP 2: Data Governance Framework Report
Develop Data Protection Model	WP3: i. Provisioning Security in A Next Generation Mobility as a Service System, paper accepted at 7th Conference on Internet of Things, Big Data and Security (IoTBDS 2022), ii. User Configurable Privacy Requirements Elicitation in Cyber-Physical Systems, paper accepted at 30th ACM Conference on User Modeling, Adaptation and Personalization (UMAP 2022).
Integrate Data Governance Framework and Data Protection Model	WP 4: Service Layer Models
Dissemination	(a) Publication of Results in peer reviewed publications, and (b) Dissemination at PETRAS events

3. DESCRIPTION OF PROJECT WORK, SUMMARY OF PROGRESS MADE, AND ACCOMPLISHMENTS

The project work was divided into five major tasks, viz:

Task 1: The first tranche of work initiated and completed was the elicitation, capturing, and collating of stakeholders' requirements in a MaaS ecosystem. Potential stakeholders of a MaaS system are quite vast, and may include: the MaaS provider, passengers of transport services, the Transport Authority regulating transport services, transport service providers, payment providers, ticketing providers, tracking providers monitoring the status of vehicles, stations, stops and luggage, and potentially cloud providers for data storage, computation, policy enforcement, mobile application providers, travel insurance providers, etc. Some of the collated requirements were from published resources. We also took advantage of the in-house expertise of the Civil Engineering staff that were members of the UMIS team, to elicit and capture more requirements.

The deliverable of this work was the UMIS Stakeholders User Requirements Report. The elicited requirements formed part of the inputs of the investigation and development of the Data Governance Framework, as well as the development of the Data Protection Model. Another significant finding of this work was our development of user stories in a MaaS ecosystem, which led to our work in the demarcation of these stories into scenarios, that we believe, are generic enough to be usable and applicable in other transportation domains. These scenarios have been included in the aforementioned Requirements Report.

The outputs of this task fulfils one of UMIS' research objectives of capturing salient requirements of MaaS stakeholders.

Task 2: The second task involved the investigation and development of the Data Governance Framework. Here, by investigating other data privacy frameworks, such as SDM [S5], CNIL [S6], and LINDDUN [S7], we developed the UMIS Data Governance Framework that focussed on the data protection goals of: Data minimisation, Confidentiality, Integrity, Availability, Unlinkability, Transparency, and Intervenability; together with risk assessment properties of a threat's Likelihood, Impact, and Severity. These were also combined with the mitigation controls of Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of Information, Unawareness, and Non-compliance. This Data Governance Framework was then applied to some of the MaaS scenarios developed as part of Task 1. The Data Governance Framework laid the foundations for lawful and secure processing of MaaS data, both for the data producers as well as the consumers. This framework, and the foundations it helped to lay, fulfils one of the UMIS' research objectives of: (a) building in of privacy in the data production and consumption of MaaS entities, and (b) ensuring that the processing, inferencing, and analytics performed on data of MaaS' users do not lead to the diminution of that data's privacy.

Task 3: The third task focussed on the development of the Data Protection Model. This task made use of the stakeholders' requirements from Task 1, plus outputs of the Data Governance Framework for the investigation and the development of the Data Protection model. The investigation in this task consisted of two sub-tasks: (a) using STRIDE Threat Modeling framework [S8] to analyse security threats were Task 1's stakeholders' requirements enacted, and also developing subsequent mitigations against these threats; and (b) using LINDDUN privacy analysis framework to analyse the privacy threats if stakeholders' requirements from Task 1 were enacted. The Data Governance Framework from Task 2 gave an overarching background to the use and application of both STRIDE and LINDDUN methodologies.

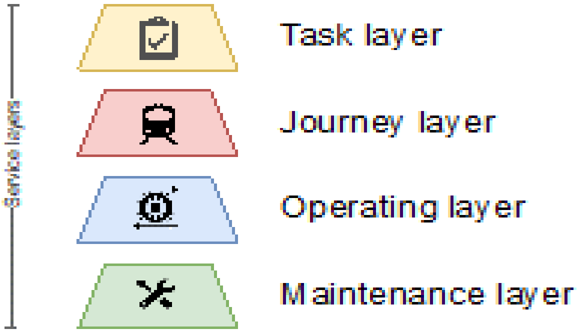

Figure 2 - The Four Layers of a MaaS system

Task 4: This task focussed on the integration of the Data Governance Framework with the Data Protection Model. In enacting this task, we applied the concept of **Activity Theory** [S4] to guide us in this integration. Activity Theory enabled us to introduce a **Service Layer** architecture into the operational structure of a MaaS environment. Consequently, we were able to delineate the operations of the stakeholders of a MaaS system into four layers (figure 2). These layers are:

Layer 1: **The Task Layer** captures the objective of a user's activity. Oftentimes, in current mobility systems, this layer exists in the mind of the end-user only; therefore, it is not necessarily enhanced or impinged upon by data processing. Once the end-user shares information about her objectives to services, these services become additional services. Additional services are services that are intended to offer additional value (related to quality of service) to the end-user, in particular in the light of the objective(s) of the end-user. These services are not considered to be subordinated to services within other layers.

Layer 2: The Primary service layer covers the processing activities performed by a "primary service", the performance of which is triggered by the request of the end user (irrespective of her motive). It includes the transport service and associated processing activities like payment clearing and ticket creation. Primary services typically require access to individual-level personal data and most likely personal identifiers, be they direct or only indirect. The intended processing impact is individual impact and as illustrated below a wide range of unwanted harms could follow as a result of the exploitation of the personal data. The intensity of the societal harm is however probably lower for this layer than for the task layer.

Layer 3: The Operating layer. The Operating layer covers sub-services that are necessary for the day-to-day operations of the primary services, but are not specifically triggered by the end-user. For example, traffic control on train platforms. Processing for these secondary services usually focus on the big picture. Taking the example of traffic control, a traffic manager will need access to the volume of passengers boarding the service but not to their identities. Whereas data at the Primary Service layer may encompass a whole journey, the Operating layer is more likely to operate on a particular leg of the journey. For example, a taxi operator may process pick-up and drop-off points for an airport transfer, but need not know details of the flight that preceded the transfer. Processing within the Operating layer will usually be performed upon aggregated data. Secondary services are intended to produce operational impact but could still generate mental harm, harm to dignity or societal harm.

Layer 4: The Maintenance Layer. The Maintenance layer covers secondary services, i.e., services necessary for the medium and long-term sustainability of the Primary Service and Operating layers, e.g., the maintenance of the IT infrastructure. These services contribute to the sustainability of the primary service. Processing for the services within the Maintenance layer does not typically need access to individual-level personal data related to end-users. Secondary services are likely to require access to non-personal data, i.e. data that does not relate to individuals. For example, maintenance of a transport provider’s fleet needs access to data that relates to vehicles, but not to personal data about the passengers. Analytics for platform optimisation, which is another typical use within the maintenance layer, should be performed upon aggregated data only. The intended processing impact of services within this layer is therefore collective impact. Unwanted societal harm could be associated with such an impact.

These Service Layers form a top-down structure. Each layer represents a data profile, with each data profile containing information on the data needs of the services captured by that layer. Higher-level layers depend on the lower-level layers to operate but also enjoy greater level of access to personal data. Participating stakeholders subscribe to the layers that cover the services they provide. A stakeholder may operate several services, each belonging to a different layer. The layers express the data needs of the services they cover and govern how sharing of data between services will be performed. Services within the same layer will enjoy access to the same category and profile of data for that layer.

By externalizing the data needs of the services of each layer, it allows participants, including data consumers, to be cognizant of the type of data for the services and also for that layer. This form of data profile explicitness and awareness help to grow trust, especially within MaaS data consumers, of how data are being produced, used, and shared.

Task 5: Speculative Legal Design in Action. In this task, we went further by applying a “speculative design” approach to re-imagine legal interpretations of data protection principles within a MaaS use case. Speculative Design “describes critically oriented research practices that create artefacts, representations, or depictions of possible and often alternate futures, removed from immediate practical concerns of implementation and commercial viability." [S10] Speculative Design is a forward-looking branch of Design which consists in hypothesising future artefacts to assess how they might affect individuals and communities in the future. Speculative Design lives within the realm of the plausible and the possible to find alternatives to the probable, i.e., what is likely to happen based on how techno-social systems are built today, with a view to informing the definition of the preferable at a later stage.

Speculative Legal Design involves at least four iterative steps: (a) Discover, i.e., the discovery of the ecosystem in which the user will operate, (b) Define, i.e., the problem statement related to the operationalisation of the user-centric system to be built and associated user needs, (c) Ideate, i.e., the sketching of the architecture of the system through which users will operate or interact, and (d) Assess, i.e., the assessment of the implications of the compliance stance adopted to sustain the user-centric system ideated in the previous step.

In Task 5, we showed how design thinking, especially its four stages (of Discovering, Defining, Ideating, and Assessing), can be applied to understanding and defining the legal challenges in a typically data intensive IoT (MaaS) environment. We used the four layers of our Service Layer Model to design a data protection enhancing service architecture for a MaaS ecosystem, while the design of the service architecture was driven by both Service Design and data protection goals. The ideation process encouraged us to introduce the concept of service divisibility to group business activities into categories associated with a data need[1], a set of processing activities and impacts to give substance to the concepts of purpose limitation and legal basis.

By applying Speculative Legal Design in Action, we were able to associate legal bases to the processing activities occurring within a MaaS ecosystem and, by utilising the layering principle of our Service Layer Model, noticed that some legal bases were more suitable depending upon the services provisioned and/or delivered in that layer (Table 2).

Table 2: Allocation of Legal Bases per Layer

Service Layer	**Legal Bases**
Task Layer	Consent
Primary Service Layer	Performance of a contract
Operating Layer	Legitimate Interest
Maintenance Layer	Legitimate Interest

[1] A data need can be described as the volume of and types of data that are necessary for a service owner acting as a data consumer to process the data and to provision and/or deliver the service.

For example, the performance of a contract legal basis is better suited for the Primary Service layer; as the services belonging to this layer are core services, meaning they execute an end user request or are an expression of the end user's need (e.g., transport me from A to B). They are thus contractually necessary for the performance of the contract concluded between the end users and the transport service provider.

However, as regards both the Operating and the Maintenance layers, the legitimate interest legal basis appears to be more apposite to the services in these two layers. When it comes to the Task Layer, we noticed that consent is the most appropriate legal basis.

The Data Governance Framework, the Data Protection Model, the Service Layer architecture, together with the Speculative Design in Action response. provides a way that MaaS ecosystem partners, including members of the general public, can participate in the trustworthy production, consumption and sharing of data thus ensuring the privacy of their data, both at rest and in motion.

By focusing upon the design of a privacy-by-design service architecture, we have generated a set of meta principles that help accelerate the operationalisation of data protection compliance in the context of a multi-party data sharing ecosystem (such as we have in a MaaS system). This definition of service layers, informed by core data protection principles such as purpose limitation, data minimisation, the least privilege principles, allowed us to specify data needs for each layer, data sharing restrictions across layers, and impact narratives for each layer. By adopting a user-centric approach, this service architecture blueprint enabled us to define a hybrid data governance model combining both centralising and decentralising.

Two of our results are highly apposite for policy makers. These are our: (1) Data Governance Framework deliverable, and (2) our deliverable titled "Speculative Legal Design in Action".

Although we were unable to implement our model on real data, as one of our partners, Solent Transport, were unable to supply us with data of users of their transportation services, most of the project objectives have been reached.

UMIS was able to combine the domains of Law, Civil Engineering, and Computer Science into solving a very important issue, data privacy, in a very visible and modern transportation infrastructure, MaaS. We were able to find common grounds from experts of the three fields. We were also able to ask pertinent questions and through that provided solutions that are applicable in industry.

4. USER PARTNER ENGAGEMENT UPDATE

UMIS had four partners involved, one of which is an academic institution, The University of Southampton. The other three partners involved were: KnowNow, Immuta, and Solent Transport. Solent Transport are responsible for transportation services and improvements in the Solent area. Immuta builds legal engineering, data governance and compliance platforms, Immuta are looking at including UMIS framework in their trust engine. KnowNow provides a consent management platform, Consentua, that enables trustworthy customer journey and user experience, and are looking at including UMIS framework in Consentua. Although, we were not able to fully engage with Solent Transport during the project's duration, we were very closely engaged with Immuta and KnowNow throughout, working with them and meeting with them, once every week.

Immuta and KnowNow are poised to drive change related to the outputs of UMIS.

5. PATHWAYS TO IMPACT

The current implementation of MaaS systems is characterised by: a surfeit of data generation and consumption, as well as multi-party data sharing, especially between data producers. Notably, these data generation and multi-party data sharing are inherently opaque to data consumers. And, embedded in these are lack of transparency and traceability of data flows.

UMIS produced a Data Governance model, grounded in theory, which can inform the design of trustworthy MaaS ecosystems, in terms of their data economy, in a way that accords with GDPR. Through our novel Service Layer architecture, we showed how our approach can support modelling of complex MaaS systems by providing a user-centred understanding of privacy and security risk levels.

Our Data Governance model, and the Security and Privacy frameworks developed in the project, will help guide MaaS ecosystem partners in the provisioning of security and privacy for the data being produced, consumed, and shared on their platforms, eventually leading to the emergence of trustworthy MaaS services. In addition, data consumers will benefit from having their fundamental rights respected as they use future transport systems.

Our results can be used by other data intensive IoT domains, such as Health, Foods, and the Construction industries, as a model (or guideline) that can be followed to provide sound data security and privacy in their domains.

6. BIGGEST CHALLENGES PROJECT FACED AND HOW THEY WERE TACKLED

The biggest challenge we faced was the inability to engage Solent Transport, fully, and the consequent inability to be able to use real life data to test our models. We were able to mitigate this challenge by drawing on the domain experience of the Civil Engineering Academic, of the University, that are members of UMIS.

7. EXTERNAL INFORMATION AND OTHER ACTIVITIES

The major part of our dissemination has been through publications of our results in peer-reviewed journals. We published our results at the 7th Conference on Internet of Things, Big Data and Security (IoTBDS 2022) and at the 30th ACM Conference on User Modeling, Adaptation and Personalization (UMAP 2022). We also participated in most of PETRAS' conferences, where we were able to apprise colleagues within PETRAS of our work and results.

8. CONCLUSIONS

UMIS brought together ideas and expertise, in Law, Civil Engineering, and Computer Science, to solving an important issue in Cybersecurity in a data intensive IoT environment. That important issue is data privacy, especially how data privacy of data producers and consumers be protected and respected in a Mobility-as-a-Service (MaaS) system. We delivered a Data Governance model that can help facilitate security and privacy of data production and consumption in such systems. We also provided Security and Privacy frameworks that help undergird this model. These two frameworks have been published in peer-reviewed journals. In addition, by applying the concept of Activity Theory, we delineated a complex ecosystem such as MaaS into Service Layers of four: (i) Task Layer, (ii) Primary Service Layer, (iii) Operation Layer, and (iv) Maintenance Layer. We showed how these Service Layers can be used to enabling and engender the protection and privacy of data in an IoT environment. Our unique combination of Civil Engineering, Law and Computer Science strengthened the project allowing us to explore important questions in the intersection of data protection, privacy regulations and resilience in MaaS systems in particular, and civil infrastructures and the Internet of Things (IoT), in general.

We will pursue our speculative legal analysis approach further. Our use of activity theory to describe MaaS system layers has provided an interesting case study for further development of multi-stakeholder activity theory which can lead to clearer separation of concerns of data security and privacy provisioning amongst the partners, which we will continue to develop. We will make use of MaaS case study insights in future planned proposals around participatory data governance approaches.

9. REFERENCES

[S1] 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

[S2] Maple, C., Wakenshaw, S., & Taddeo, M. (2019). "Privacy and Trust Stream", Cybersecurity of the Internet of Things, PETRAS Stream Report, 2019

[S3] 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

[S4] Nardi, B.A., (Ed.). 1995. Context and Consciousness: Activity Theory and Human-Computer Interaction.

[S5] 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, 2017

[S6] Conference of the Independent Data Protection Supervisory Authorities of the Federation and the Länder, The Standard Data Protection Model (v 2,0b, 17 April 2020) https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V2.0b.pdf

[S7] CNIL, Privacy Impact Assessment (PIA): Methodology (February 2018) https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf

[S8] Deng, M., Wuyts, K., Scandariato, R., Preneel, B., and Joosen, W., (2011). A privacy threat analysis framework: Supporting the elicitation and fulfilment of privacy requirements. Requir. Eng. 16 (03 2011), 3–32. https://doi.org/10.1007/s00766-010-0115-7

[S9] Shostack, A. (2014). Threat Modeling: Designing for Security.

[S10] Wong R.Y., Khovanskaya V. (2018) Speculative Design in HCI: From Corporate Imaginations to Critical Orientations. In: Filimowicz M., Tzankova V. (eds) New Directions in Third Wave Human - Computer Interaction: Volume 2 - Methodologies. Human – Computer Interaction Series, Springer.

All URLs were last retrieved 29th MAY 2023

APPENDICES

APPENDIX A: MORE PROJECT INFORMATION

A.1 More Project Information

Project title (with acronym): Increasing User trust in Mobility-as-a-Service IoT ecoSystem project (UMIS)

Type of PETRAS project (Catalyser/1st SRF funded etc.): PETRAS SRF 2

Project Start Date (DD/MM/DDDD): 01.07.2021

Project End Date (DD/MM/DDDD): 28.02.2023

Report Date(DD/MM/DDDD): 30/05/2023

Research Organisation(s) (Lead plus others): University of Southampton, Solent Transport, Immuta, KnowNow Information