Research in Transportation Business & Management 56 (2024) 101162

Contents lists available at ScienceDirect

Research in Transportation Business & Management

journal homepage: www.elsevier.com/locate/rtbm

The road not taken yet: A review of cyber security risks in mobility-as-a-service (MaaS) ecosystems and a research agenda

Ali Alderete Peralta [a,*], Nazmiye Balta-Ozkan [a], Shujun Li [b]

[a] School of Water, Energy and Environment, Cranfield University, Cranfield, Bedfordshire MK43 0AL, UK
[b] Institute of Cyber Security for Society (iCSS) & School of Computing, Keynes College, University of Kent, Canterbury, Kent CT2 7NP, UK

A R T I C L E I N F O

Keywords:
Integrated mobility services
Smart transport
Cyber security
Data sharing
Sustainable transport
Data governance

A B S T R A C T

This paper identifies the state-of-the-art key aspects for the development of mobility-as-a-service (MaaS) ecosystems and provides evidence on the importance of cyber security which has been broadly overlooked in the literature. The analysis is carried out in three stages: (i) a literature review, (ii) a presentation of expert workshop findings, and (iii) a synthesis of both findings to develop a research agenda on cyber security aspects of MaaS ecosystems. The review identifies and bridges the gap between two strands of MaaS literature: the studies that focus on the factors that drive the development of MaaS, and those that create narratives of future MaaS scenarios.

The analysis employs the Business Model Canvas to synthesise important factors that underline the development of MaaS in a 7-dimension matrix. This matrix is then used to assess to what extent the available MaaS scenarios cover such dimensions, showing that the literature has overlooked the incentives for users, incentives for MaaS providers, public governance and cyber security elements of the MaaS development.

Finally, this paper synthesises the findings from the review of the literature and an expert workshop to develop a research agenda to characterise and analyse the role of incentives to influence the individuals' and organisations' data sharing preferences and emerging cyber security risks in MaaS ecosystems, which will be of interest to both scholars and policymakers. Only through explicit consideration of data-sharing behaviours and risks across individuals and organisations that MaaS ecosystems can support the transition to a net-zero economy.

1. Introduction

The transport system is under constant pressure and evolution, especially in urban areas where the private car lock-in has led to a range of environmental and socio-economic problems such as congestion and carbon emissions (Butler et al., 2021). Moreover, recent global events have changed mobility and social lifestyle, hastening innovation towards more sustainable transport (Köhler et al., 2020).[1] The concept of mobility-as-a-service (MaaS) offers a significant potential to address some of these challenges by optimising the use of public transport infrastructure and facilitating seamless planning and booking in multimodal journeys (Alyavina et al., 2022; Mitropoulos et al., 2023; Utriainen & Pöllänen, 2018). The concept of MaaS was first proposed at the beginning of the 2010s, as the result of a number of smart mobility projects in Sweden and Finland (Liimatainen & Mladenović, 2018), and its definition tends to focus on different aspects of MaaS, ranging from the structure of the ecosystem (Hensher, 2017) to services and functionalities offered to the users (Enoch, 2018), and to the potential benefits for and behavioural change of users (Kamargianni et al., 2016). Although MaaS development is still in nascent phases, there is an increasing number of demonstrations in European cities (Rome, Budapest, Greater Manchester, Southern England, or Luxembourg city) (Alyavina et al., 2022; Jittrapirom et al., 2017; Kamargianni et al., 2016; Mitropoulos et al., 2023; University of Southampton, 2024; Utriainen & Pöllänen, 2018), with initiatives such as the MaaS Alliance in Europe (MaaS, 2021), or research on MaaS acceptability and development in the UK (Bizgan et al., 2020; Department of Transport, 2020). Nevertheless, there are still a number of barriers to their development, including the lack of willingness of private and public organisations to cooperate (Vaddadi et al., 2020), the lack of regulations to ensure fair competition while promoting data sharing (Zöschinger, 2019) as well as to protect the integrity of users' digital data (Stringer, 2018).

* Corresponding author.
E-mail addresses: a.aldereteperalt@cranfield.ac.uk (A. Alderete Peralta), n.ozkan@cranfield.ac.uk (N. Balta-Ozkan), S.J.Li@kent.ac.uk (S. Li).

[1] The United nations recognises the key role of sustainable transport in Sustainable Development Goals 3, 9 and 11 (United Nations, 2017).

https://doi.org/10.1016/j.rtbm.2024.101162
Received 11 July 2023; Received in revised form 28 March 2024; Accepted 17 June 2024
Available online 1 August 2024

The importance of data sharing and the role of different actors are noted by a number of scholars. Pangbourne et al. (Pangbourne et al., 2020) point out that the development of MaaS is a complex socio-technical phenomenon that results in non-linear pathways, which are difficult to predict and whose complexity is constantly increasing due to the incorporation of new technologies and actors. They also mention that the transport system's actors interact through physical, social or business networks which comprise data sharing between public and private actors and users and may lead to the emergence of cyber security risks for all parties involved. In another work, Pangbourne et al. (Pangbourne et al., 2018) note how the high dependence of MaaS ecosystems on information and communication technologies (ICTs) may cause a disruption in the transport system in the case of deliberate cyber attacks such as denial of service (DoS) attacks. Butler et al.'s review (Butler et al., 2021) identifies a list of potential risks that may emerge from the integration of transport services, including social inequity, data monopolisation and cyber security, the last of which applies to both users and service providers. For instance, financial or travel data breaches may represent a risk for competitiveness if a service provider's intellectual property on how such data is collected and used technically is breached (Butler et al., 2021).

Undoubtedly, the above-mentioned insights about cyber security risks may inform the development of preventive strategies to mitigate such risks. However, the discussion on what cyber security risks may emerge for users and service providers in a MaaS ecosystem is scarce in the literature (Pangbourne et al., 2018). To our surprise, cyber security risks are also overlooked in studies that portray MaaS scenarios of the future. The increasingly growing literature outlining potential pathways for transition to a MaaS ecosystem has focused almost only on the level of functionalities (Liimatainen & Mladenović, 2018; Utriainen & Pöllänen, 2018) and information integration (Hensher, 2017; Köhler et al., 2020), rather than cyber security risks and countermeasures.

The lack of sufficient consideration of cyber security aspects in MaaS-related research is worrying. This becomes even more so if we consider the fact that real-world cyber security problems and solutions involve a wide range of socio-technical aspects and trade-offs between conflicting requirements (Angela Sasse & Rashid, 2019; Burnap, 2019), e.g., more secure solutions can be difficult to use, expensive to operate, and could conflict with intrinsic (not security-related) functionalities. Looking beyond transport systems, the types, scale and importance of cyber security risks can be seen in other sectors like online banking. It is estimated that the impact of these risks can reach 0.4–1.5% of global GDP. In the financial sector, the intersection of technologies, processes, and individuals gives place to the emergence of cyber security threats (Kurmanova et al., 2021), requiring organisational change from all the stakeholders involved (Buckley et al., 2019). This results in cyber security being one of the relevant barriers to online banking [Singhal] [Aladwani]. On the other hand, discussion of cyber security risks for the MaaS ecosystem is scarce and mostly limited to data privacy. While, to the best of our knowledge, there are no reported cases of cyber security incidents in the current MaaS schemes, one could argue that similar threats and cyber attacks may emerge for MaaS. Indeed, with increasing digitisation, Kurmanova et al. (Kurmanova et al., 2021) report that, by 2019, cyber crime and cyber security risks are in the top five global risk challenges for every organisation.

For cyber-physical systems such as MaaS, the complexity of cyber security problems and solutions is even higher, because of the number of single organisations collaborating in the ecosystem (Cardenas & Cruz, 2019; Habibzadeh et al., 2019). This calls for highly interdisciplinary research that carefully considers all key stakeholders and system components. To understand the complexity of the MaaS ecosystem, one can have a look at the different business models for the MaaS providers (i.e. (Corazza & Carassiti, 2021; Polydoropoulou et al., 2020)). These comprise several items and dimensions with complex relationships. However, as further discussed in this paper, the scenarios for MaaS development found in the literature are rather simple, focusing on only a few of the important building blocks as dimensions for their narrative.

As illustrated in Fig. 1, the MaaS literature can be divided into two strands: the studies that focus on the factors that drive the development of MaaS, and those that create narratives of possible future scenarios for MaaS. Yet, there is a disconnect between these two strands, resulting in scenarios that fail to inform what factors are required to move from the current state to the desired scenarios in the future. The novelty of this paper is to bridge the gap between these two strands, by developing a 7-dimensional matrix that can be used to assess the maturity of MaaS ecosystems and the coverage of future MaaS scenarios. This matrix emerges from the synthesis of academic and grey literature[2] for relevant factors that underline the development of MaaS. A second contribution is the assessment of available MaaS scenarios mainly to incorporate three of these dimensions (ecosystem integration, organisational transition, platform functionality) while overlooking the remaining ones, i.e. incentives for users, incentives for MaaS providers, public governance and cyber security. As shown further in this paper, cyber security risks are largely ignored in many studies. Using these published MaaS scenarios (Cisterna et al., 2021; Cisterna et al., 2022; Enoch, 2018; Enoch et al., 2020; Smith, Sochor, & Karlsson, 2018a; Vaddadi et al., 2020; Wong et al., 2020), we identify key cyber security risks that need to be considered in future research. Then, to address the scarcity of MaaS scenarios for the UK, these insights were contextualised for the UK at an expert workshop with participants from the industry, the public sector, and academia.

Through a review of the literature and utilising discussions from an expert workshop, this paper aims to identify the nature and characteristics of cyber security risks associated with the development of MaaS, to fill the identified research gaps mentioned above. In particular, it has the following objectives:

1. to create a MaaS development matrix considering all important dimensions including cyber security, and to assess the coverage of these dimensions in the reviewed MaaS scenarios,

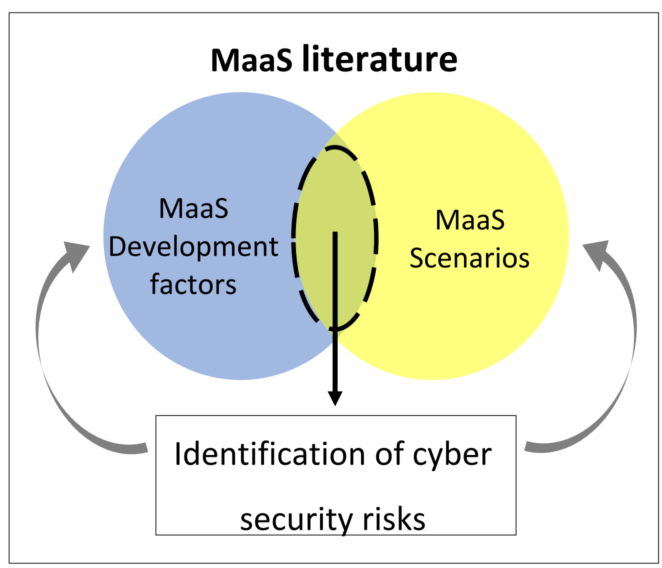

Fig. 1. A conceptual framework to identify the gap in cyber security risks in theMaaS literature.

[2] There is a variety of definitions for grey literature (Mahood et al., 2014; Mering, 2018), in this paper we consider publicly available online articles or government reports that may have not been peer-reviewed.

2. to evaluate and validate the relevance of identified cyber security risks in selected MaaS scenarios for the UK context via an expert workshop, and
3. to suggest a research agenda for the incorporation of cyber security risks in MaaS ecosystems.

The rest of this paper unfolds as follows. Section 2 introduces the methods we use for the review, whilst the results are presented in Section 3. Section 4 discusses the research gaps and proposes a research agenda based on our findings. Finally, Section 5 presents a summary of our findings and a conclusion.

2. Methods

This paper develops a research agenda for the analysis and further understanding of cyber security risks related to MaaS. Fig. 2 displays the research process, which is composed of three stages: (i) a literature review, (ii) an expert workshop, and (iii) a discussion and synthesis of findings. The review develops a seven-dimensional (7-D) matrix that synthesises important factors that underline the development of MaaS identified in the academic and grey literature. This matrix is then used to identify whether selected state-of-the-art future MaaS scenarios consider these dimensions. Then, these insights are contextualised for the UK at an expert workshop with participants from the industry, the public sector, and academia. Finally, this paper proposes potential avenues for further research.

The first stage aims to identify relevant factors that affect the development of MaaS. The review adopts a systematic umbrella review (review of reviews) (Aromataris et al., 2015; Paré et al., 2015; Slim & Marquillier, 2022) and classifies such factors into a seven-dimension matrix of the MaaS development. The review also summarises the scenarios for the development of the MaaS ecosystem and uses the matrix to assess to what extent such scenarios cover each of the seven dimensions. The scope of this review covers the integration of mobility services, resulting in multimodal travel. Although, our discussion acknowledges that current mobility services present cyber security risks in their individual on-line services. Fig. 3 shows the five-step process of the literature review stage. The first step retrieves a total of 99 potential papers and only 9 were included after the title screening (the second step). During the third step, the snowballing technique was used to retrieve relevant articles cited by the 9 selected papers and increase the reliability of the review (Greenhalgh & Peacock, 2005; Sayers, 2008). Steps four and five comprise a second title screening and removing duplicates, resulting in a total of 54 articles selected. During the revision of this article, the snowballing technique was used to update the review and include recently published articles, accounting for a total of 62 articles.[3]

The scientific databases we used include Science Direct, Scopus and Google Scholar. For searches into Science Direct and Scopus, we searched into the meta data (title, abstract and keywords), and for Google Scholar we searched into the title only since the other only option (searching in full text) returned too many irrelevant items. Table 1 Summarises the queries made to the selected scientific databases and the inclusion and exclusion criteria at each of the review steps. Note that Google Scholar did not support nested search queries, so we split the search queries into a number of simpler queries to get the candidate papers.

The second stage of our work comprises an expert workshop that aims to put the results from the literature review in the UK context. The workshop had the following objectives:

1. to help inform the future research agenda on making MaaS ecosystems more secure for all participating actors,
2. to identify common cyber security risks in selected MaaS scenarios, considering relevant business models and cyber security-related behaviours of people and organisations, and
3. to gather the requirements, preferences, wishes and intents of the participants to collaborate on the research agenda.

At the workshop, the participants were first presented with a summary of findings from the literature review and our initial assessment of future MaaS scenarios. Then, through a facilitated open discussion, we aimed to collect evidence and individual experiences regarding cyber security risks related to the integration of transport services into a single platform.

In the last stage of our work, we focused on synthesising findings from the literature review and the expert workshop to propose a research agenda.

3. Results

3.1. Review of MaaS development factors

We first present a review of the MaaS development factors using the Business Model Canvas (BMC) proposed by (Corazza & Carassiti, 2021; Polydoropoulou et al., 2020), which exemplifies the elements considered in a MaaS ecosystem. The authors describe the structure of the value proposition for four European MaaS ecosystems (Rome, Budapest, Greater Manchester, and Luxembourg City). These BMCs identify an extensive list of 34 factors for the development of MaaS that are grouped into nine building blocks (see Fig. 4).Table 3, in Appendix A, groups the different MaaS elements used in both literature strands according to the BMC's factor and building block.

However, the BMC doesn't offer clarity on whether any of those factors act as drivers and barriers nor how they are linked to each other. To reduce ambiguity and elusiveness in the use of these 34 factors, we propose grouping these into 7-dimensions (7-D) to consider their interaction and interdependencies as follows: ecosystem integration, organisational transition, platform functionality, incentives for users, incentives for operators, public governance, and cyber security.

3.2. Seven-dimensional MaaS development matrix

Table 2 lists the 7-D and provides a brief description. For instance, **Dimension 1: Ecosystem integration** emerges from studies that present a narrative on how the number of travel modes available in the platform reflects the maturity level of the ecosystem (Corazza & Carassiti, 2021). The number of travel modes has also been used to reflect the openness of public and private providers to share their data within the MaaS ecosystem (Vaddadi et al., 2020). Other authors classify the MaaS ecosystem based on the level of integration (Kamargianni et al., 2016; Pangbourne et al., 2020), while Zhao et al (Zhao et al., 2020) point out that a barrier to the success of the MaaS ecosystem is the lack of integration between private and public transport. As seen in Fig. 5, this dimension mostly covers the "Key Partners" building block presented in the BMC, but also includes factors from the "Customer Relationships", "Customer Segments" and"Key Resources". We argue that our classification helps avoid overlapping narrative elements when using the BMC towards designing scenarios of MaaS development. The distribution of BMC's factor and building blocks across the 7-D is listed in Table 3 in Appendix A, showing also whether these factors have been considered in both of the MaaS literature's strands.

This concept has been utilised by MaaS scholars, including Vitkauskaite and Vaiciukynaite (Vitkauskaite & Vaiciukynaite, 2020), to compare four shared micro-mobility services in Europe.

Two key findings of Fig. 6 and Table 4 are that Ecosystem Integration, Platform Functionality, and Organisational Transition dimensions have been widely studied in the literature. On the contrary, Incentives for Users, Incentives for MaaS providers, Public Governance and Cyber

[3] * The second round of snowballing is not included in Fig. 3 to represent the original methodology.

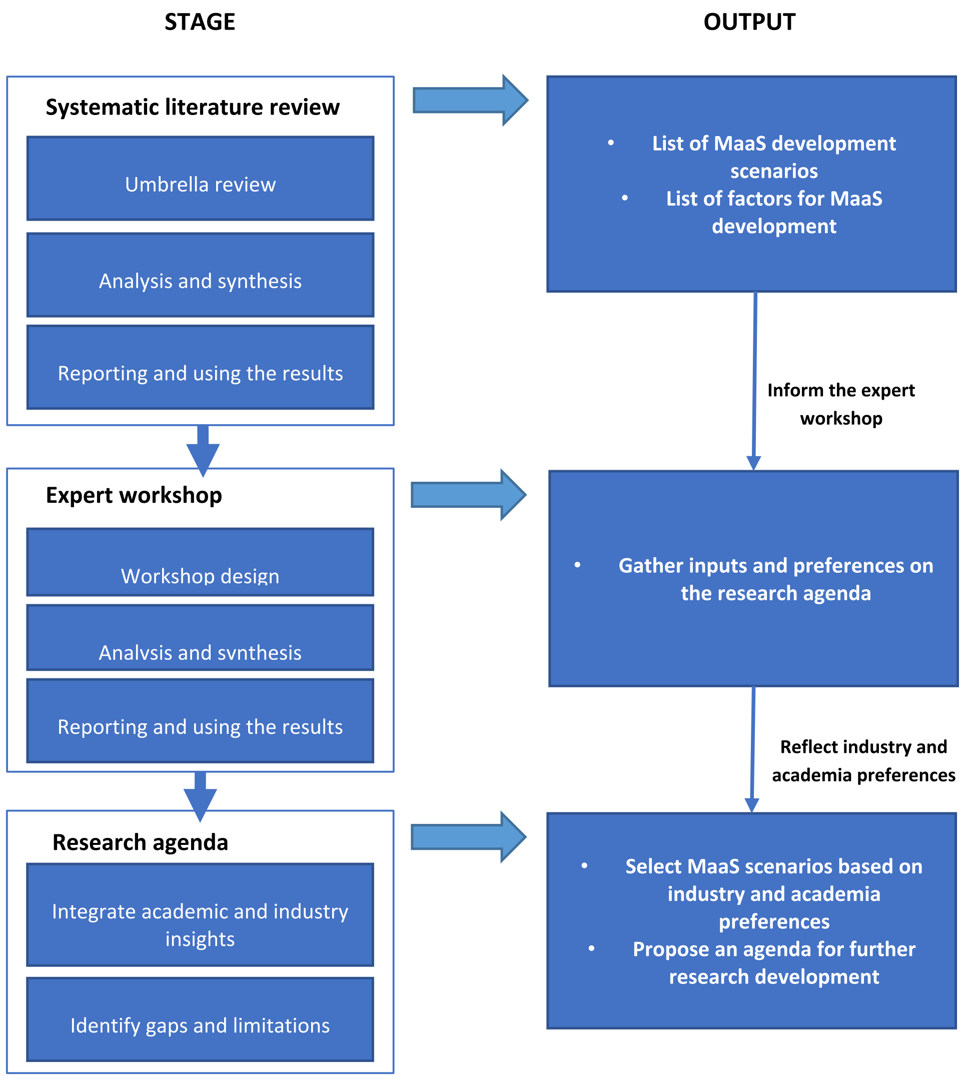

Fig. 2. A three-stage methodology for developing a research agenda.

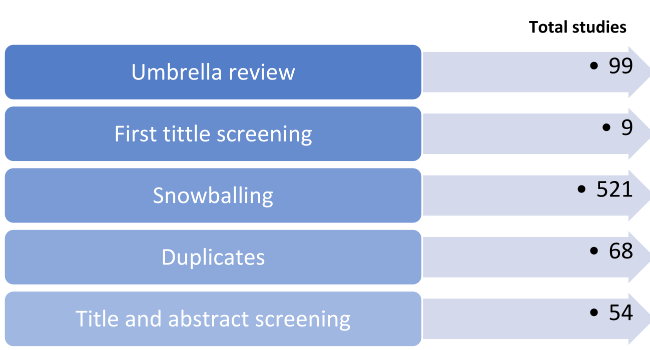

Fig. 3. A five-step systematic literature review process.

Security are areas that received limited attention. This finding is consistent across both literature strands. A second finding is that the number of studies and coverage of MaaS elements is limited for the MaaS scenarios literature, in comparison with the other literature strand. For ease of reference and visual aid, our 7-D matrix and its constituents are presented in Fig. 6. Each of these dimensions is presented in detail below, though our main focus is identifying how the cyber security dimension interacts with the other six.

3.2.1. Dimension 1: MaaS ecosystem integration

The level of ecosystem integration has been used as a maturity metric for the MaaS ecosystem (Corazza & Carassiti, 2021; Utriainen & Pöllänen, 2018), yet, the literature does not agree with what is the required integration level to consider a transport system as a MaaS ecosystem (Alyavina et al., 2022). The concept of integration has been studied from different perspectives, for instance, Vaddadi et al. (Vaddadi et al., 2020) discussed the effect of integrating data from the different public transport suppliers on the uptake of MaaS as technology innovation. Other researchers looked at this from the physical, policy and sectorial views (Corazza & Carassiti, 2021), the functionality of the system or application (Kamargianni et al., 2016; Stringer, 2018), or the role of previously existing systems that lead to an integrated system (Pangbourne et al., 2020).

Zhao et al. (Zhao et al., 2020) analysed the case of a corporate MaaS service for a company's employees, which facilitates mobility for employees within, to and from the company sites. The service comprises internal taxis, small shuttle buses and shared e-bikes available in the company area. However, because this private service fails to connect with public transport, the service planning capabilities are limited resulting in being unappealing for the users (Zhao et al., 2020). In line with these results, Vaddadi et al. (Vaddadi et al., 2020) suggested that when public transport is not willing to share their data with the MaaS provider, private services (e.g., car-based services) tend to dominate the

Table 1
Review elements: query, inclusion, and exclusion criteria.

Stage	Criteria
Umbrella review	("mobility as a service" OR "maas" OR "mobility service" OR "mobility-as-a-service" OR "integrated mobility service" OR "mobility integration") **Subject areas included for Science Direct:** Social Science, Engineering, Computer science, Environmental science, Energy, Business, Management and Accounting, Mathematics, Decision Science, Neuroscience, and Undefined.
First title screening	**Exclusion** • Articles not related to transport • Articles related to a single transport modality or transport-related technology, e.g., e-scooters or autonomous vehicle integration
Snowballing	**Forwards**: articles that cite an already selected article were analysed. These articles were screened considering the first title screening criteria. **Backwards**: articles cited by an already selected article were also screened. These articles were screened considering the first title screening criteria.
Duplicates	**Duplicates** were identified via title comparison, and then only one paper was kept among all duplicates.
Title and abstract screening	**Inclusion** • Review of MaaS scenarios • Review of current MaaS schemes • Theoretical MaaS business models

market. On the other hand, when public transport is willing to share their information, the users are offered seamlessly integrated mobility services and help MaaS take over the market. The main barriers to ecosystem integration are the available policies and geographical boundaries. Vaddadi et al. (Vaddadi et al., 2020) highlight that those private services are willing to share their data only on a limited basis due to conflicting interests with their competitors. Also, they point out that private services are profit-focussed and they may offer packages that are not necessarily the best for societal good. Such packages are likely to be car-based services, thus, in principle, this is against some of the key expected benefits of MaaS (e.g., reducing carbon emissions via less dependency on cars) (Jittrapirom et al., 2020; Utriainen & Pöllänen, 2018).

Tinnilä (Tinnilä, 2016) discusses how the bundling of uninterrupted and connected multi-modal services is the main element and difference between MaaS and traditional transport services. They note that the scope of integrated services goes beyond the transport network and the transport operators to include private cars, parking facilities, and traffic monitoring systems. Because these elements are public and private, the centralisation of services and infrastructure represents a challenge for the MaaS provider (Tinnilä, 2016).

Corazza and Carassiti (Corazza & Carassiti, 2021) mentioned that integration is not a new concept in the urban mobility domain and that this works at the physical, policy and more recently at the actors' level. Additionally, the authors highlight that the MaaS requires a degree of data sharing, which is contingent upon cooperation among the transport operators, technical components (ICTs), and regulatory frameworks. Kamargianni (Kamargianni et al., 2016) reported on three main elements of the MaaS ecosystem: ticketing and payment, modal options and online interfaces. Then again, they acknowledge that integration is not a novel concept and list a vast number of examples such as smart cards, an example of which is Transport for London's Oyster card. Then, Kamargianni et al. (Kamargianni et al., 2016) defined three levels of integration: partial, advanced without mobility packages, and advanced with mobility packages. They demonstrate how a higher level of integration

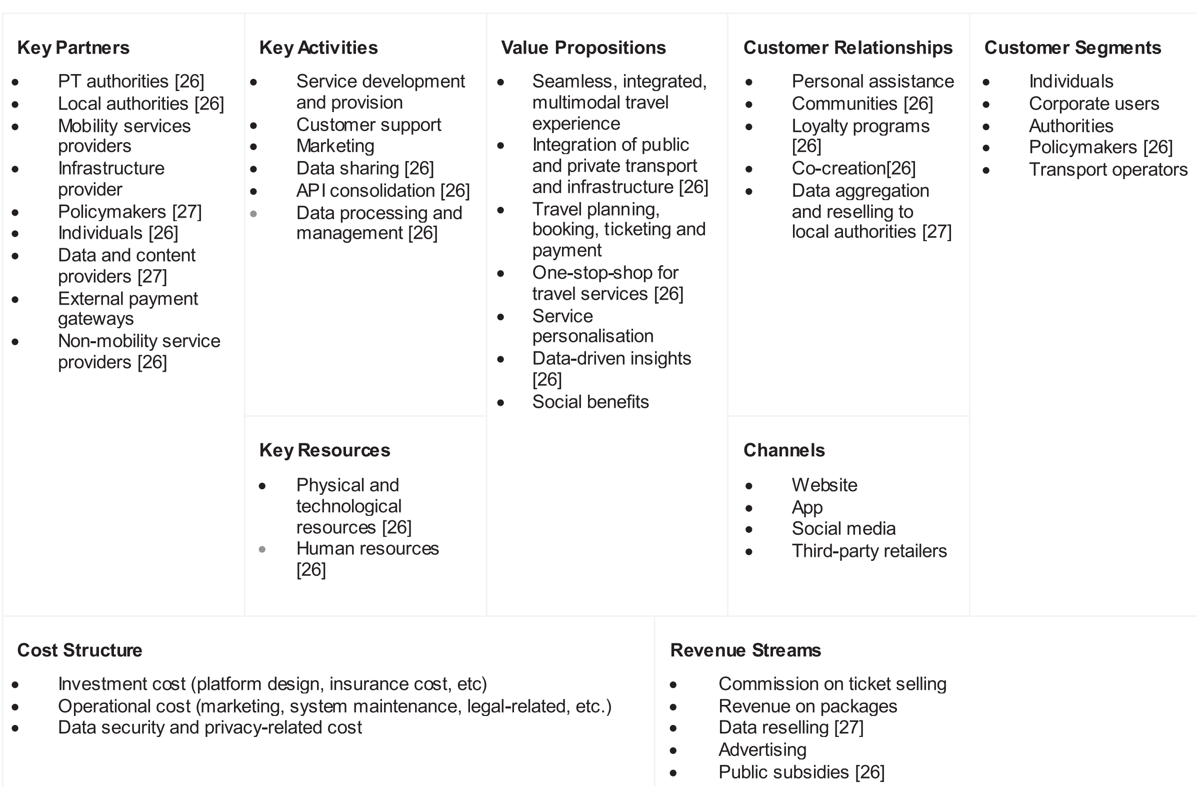

Fig. 4. The business model canvas for MaaS.
Adapted from: Polydoropoulou et al. (Polydoropoulou et al., 2020) and Corazza and Carassiti (Corazza & Carassiti, 2021); each element is common to both canvases, except if indicated.

Table 2
Definition of our seven-dimensional MaaS development matrix.

Dimension	Definition	References	Total (48)
Ecosystem integration	The openness of stakeholders to share their data reflects on the number of modes available.	(Corazza & Carassiti, 2021; Enoch, 2018; Enoch & Potter, 2023; Kamargianni et al., 2016; Mitropoulos et al., 2023; Pangbourne et al., 2020; Stringer, 2018; Tinnilä, 2016; Vaddadi et al., 2020; Wong et al., 2020; Zhao et al., 2020)	11
Organisational transition	Required changes on the current business models, i.e., reselling tickets.	(Corazza & Carassiti, 2021; Duan et al., 2022; Mitropoulos et al., 2023; Smith, Sochor, & Karlsson, 2018a; Smith, Sochor, & Sarasini, 2018b; Smith & Sørensen, 2023)	6
Platform functionality	Real-time information, trip planning, booking, e-ticket, e-payment, etc.	(Corazza & Carassiti, 2021; Enoch et al., 2020; Enoch & Potter, 2023; Kamargianni et al., 2016; Mitropoulos et al., 2023; Mulley, 2017; Smith, Sochor, & Sarasini, 2018b; Sochor et al., 2015; Stringer, 2018; Tinnilä, 2016; Vaddadi et al., 2020; Vitkauskaite & Vaiciukynaite, 2020; Zhao et al., 2020)	13
Incentives for users	Incentives for users offered by both the public and private sectors to increase MaaS adoption, i.e., pricing and bundling offers.	(Corazza & Carassiti, 2021; Enoch & Potter, 2023; Mitropoulos et al., 2023; Smith, Sochor, & Sarasini, 2018b; Zhao et al., 2020)	6
Incentives for operators	Programmes to increase the attractiveness to public and private sector service providers to participate in MaaS operation and scalability, i.e., transport subsidies from the central government of a nation.	(Enoch, 2018; Smith, Sochor, & Karlsson, 2018a; Smith, Sochor, & Sarasini, 2018b; Smith & Sørensen, 2023; Stringer, 2018; Vaddadi et al., 2020; Zhao et al., 2020)	8
Public governance	Policies and required changes in the regulations to ensure the public good.	(Corazza & Carassiti, 2021; Enoch, 2018; Enoch et al., 2020; Enoch & Potter, 2023; Hensher, 2017; Polydoropoulou et al., 2020; Smith, Sochor, & Karlsson, 2018a; Smith, Sochor, & Sarasini, 2018b; Smith & Sørensen, 2023; Stringer, 2018; Vaddadi et al., 2020; Zhao et al., 2020)	12
Cyber security	This includes the means to secure the transport infrastructure and MaaS processes, security and privacy of users' data	(Corazza & Carassiti, 2021; Pangbourne et al., 2018)	2

can increase the users' preference towards MaaS. Stringer reporte\d on the UK (Stringer, 2018) mentions that, besides the great work done in London to provide users with a wide multi-modal transport network system, this cannot be considered yet a MaaS because systems in place do not fully allow cross-modal point-to-point planning or payment. Pangbourne et al. (Pangbourne et al., 2020) acknowledged that MaaS is a complex socio-technical system, and as such, its development is the result of multiple actors' interactions. Pangbourne et al. (Pangbourne et al., 2020) noted that ICTs play a central role in these interactions and that MaaS is also the result of previous applications and prototypes converging into an integrated system. They listed four stages of MaaS development that have preceded the current MaaS applications: (i) ticketing and payment, (ii) peer-to-peer services (shared economy), (iii) real-time transport information, and (iv) demand response services.

3.2.2. Dimension 2: platform functionality

Although the functionality of the MaaS integrated platform is directly linked to the ecosystem level of integration, some functionalities might be key for the system to be appealing to the users. Kamargianni et al. (Kamargianni et al., 2016) noted that while mature MaaS platforms (e.g., some in Europe) usually integrate planning and booking, it is the bundling of services and product functionality that defines the most mature systems. Corazza and Carassiti (Corazza & Carassiti, 2021) also acknowledged that users respond significantly to subscriptions to multimodal mobility. The MaaS business model generates revenue directly from reselling tickets from the transport suppliers, yielding high profits against large initial investment costs incurred by the MaaS provider. Tinnilä (Tinnilä, 2016) commented on the difference in costs of such functionalities. Whilst the operation of over-the-counter services by traditional service providers is costly, the operation of digital services is very low.

While some researchers have focused on the level of MaaS maturity and the platform functionalities, Enoch et al. (Enoch et al., 2020) pointed out that users' perceptions and expectations will certainly increase while their transport needs are not likely to change substantially. They conducted a survey, which suggests that the transport services should allow the users a more effective use of time, with expectations of the transport services to be delivered almost immediately. Zhao et al. (Zhao et al., 2020) pointed out that when a new platform is deployed, the users may expect a more mature service, therefore leading to disappointment in the early stages of the service. Thus, not only the functionalities such as planning and flexibility drive the adoption of MaaS but also the users' perception of such available services.

Stringer (Stringer, 2018) noted that the MaaS scope does not finish when a user ends a journey, but there are also post-travel interactions a MaaS can provide such as parking and EV charging station payments. Similarly, Zhao et al. (Zhao et al., 2020) mentioned that the lack of routing information for walking or e-bikes (arguably last-mile modes) hinders changing the users' travel behaviours. Thus, the MaaS platform is required to provide enough information to the users about charges so that it is clear to the users what they are paying for or settle compensations if there is a disruption in the transport services (Corazza & Carassiti, 2021).

3.2.3. Dimension 3: organisational transition

It has been noted that the development of MaaS will require changes in the current business models and the operation of the public transport system. Such changes would apply to both public and private entities. For instance, Smith et al. (Smith, Sochor, & Sarasini, 2018b) discussed how governments that have deregulated the public transport sector may lead to a market-driven development of MaaS. This opens the transport sector to start-ups and innovative business models that allow reforming the transport system, whilst the public transport suppliers can focus on improving the current transport network. Others like Corazza and Carassiti (Corazza & Carassiti, 2021) also acknowledged the potential increase in the number of actors supporting MaaS services and how they interact. Their results suggest that the transition to MaaS requires the transport network actors to work in a non-hierarchical structure, rather than in the common monopoly or hierarchical way which may limit the number of transport suppliers. The authors noted that increases in the number of actors in such a non-hierarchical structure may result in more than a singular MaaS provider.

Smith et al. (Smith, Sochor, & Karlsson, 2018a) and Smith and

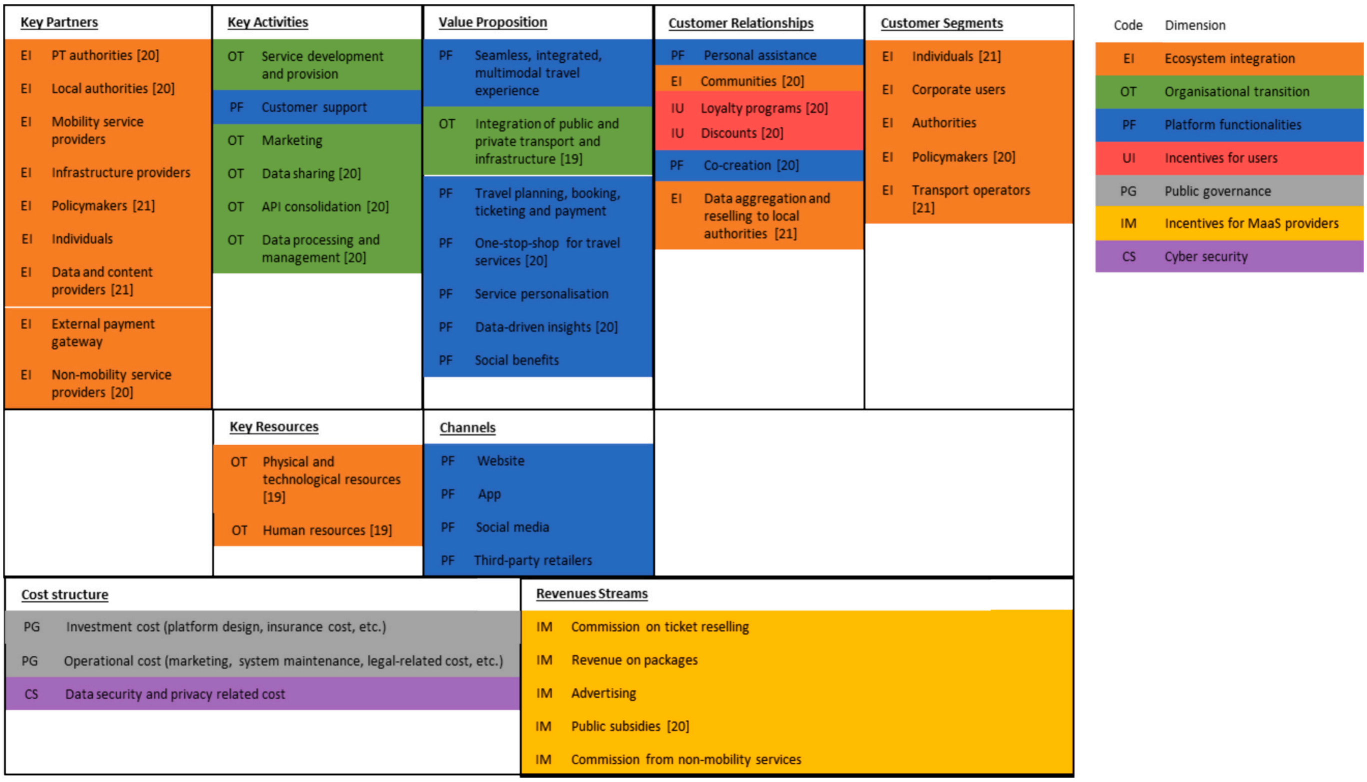

Fig. 5. Distribution of the BMC's factors across the 7 dimensions.

Sørensen (Smith & Sørensen, 2023) studied the different roles of private and public actors through three different scenarios for the MaaS ecosystem. First, if MaaS is provided by the public sector, local authorities would fund and develop the integrated transport system in liaison with private transport services such as car-sharing or -rental services. The second scenario assumes that the development of MaaS represents potential business opportunities for the private sector. Thus, MaaS is provided by a private actor such as a technology provider or a start-up company with higher ICT capabilities than the public sector. However, both studies (Smith, Sochor, & Karlsson, 2018a; Smith & Sørensen, 2023) pointed out that the public sector is required to subsidise the public transport ticket to make this business opportunity feasible for a MaaS provider. A third scenario assigns different shares of responsibility to these two sectors. Whilst the public sector liaises with the transport providers reducing the initial cost for the MaaS operator, it is still the private sector that is responsible for the ICT development and operations. It was argued that splitting the responsibilities would regulate the system better and prevent any single actor from becoming dominant. Furthermore, this would reduce the likelihood of undesired developments such as the increase of car-based services, and rather focus on the societal good.

Polydoropoulou et al. (Polydoropoulou et al., 2020) investigated the MaaS actors' motivations, noting that small organisations thrive for more exposition via working with the large companies, which in turn look after improving their understanding of customers through data (data sharing with other organisations). They also report that this difference in the MaaS actors' objectives may represent a strong barrier to cooperation and data sharing, as public actors' interest is mainly around optimising the use of public transport, whilst most private actors seek to increase their profit as the main goal.

3.2.4. Dimension 4: incentives for users

Incentives have been identified as a means to accelerate changes in users' travel behaviours (Corazza & Carassiti, 2021; Hensher, 2017; Pangbourne et al., 2018; Smith, Sochor, & Sarasini, 2018b; Stringer, 2018; Zhao et al., 2020; Zöschinger, 2019), which are usually financial in nature. However, only a few researchers name the actual format of such incentives. For instance, Matyas and Kamargianni (Matyas & Kamargianni, 2019) review some MaaS schemes that use vouchers that can be exchanged for tickets. These vouchers can be obtained by entering a lottery or collecting points. Polydoropoulou et al. (Polydoropoulou et al., 2020) highlight that such incentives are not exclusive to the scope of the transport network and can be extended to other actors. For instance, to incentivise the users to use car-sharing services, MaaS operators could include actors such as road operators and parking suppliers to arrange discount prices or loyalty schemes.

3.2.5. Dimension 5: public governance

MaaS as a concept is innately in line with sustainable development policies, nevertheless, the role of policy has been largely ignored (Corazza & Carassiti, 2021; Hensher, 2017). Smith et al. (Smith, Sochor, & Karlsson, 2018a) and Smith and Sørensen (Smith & Sørensen, 2023) also cautioned that policies and regulations may work in positive or adversarial means. Rigid and inflexible regulations may delay innovation from the private sector, whilst incomplete regulation may lead to profit-focused services. The lack of regulatory frameworks can hinder the cooperation between actors and lead to the emergence of multiple MaaS schemes, as in the case of Madrid where there are multiple MaaS initiatives (Mitropoulos et al., 2023). In the UK, the Department for Transport has published *Mobility as a Service: code of practice* [Mobility as a Service: code of practice], which pays little attention on cyber security. This document make three recommendations on Data Sharing, Data Privacy and Data quality, acknowledging that these elements impact on the development of MaaS. The recommendations cover a list of data required to share (i.e. payment data including ticket price, reservation data, timetable data, location data, carbon emissions data, etc.); to establish to stablish data sharing agreements to ensure good practice and compliance with data protection regulations (i.e Data Protection Regulation); and to set up processes to ensure the data compliances with any data standards and be able to demonstrate the accuracy of the shared

Table 3
Key characteristics of the reviewed scenarios for MaaS development.

Reference and context	Name	Description	Ecosystem integration	Organisational transition	Platform functionality	Incentives for users	Incentives for operators	Public governance	Cyber security
Cisterna et al. (Cisterna et al., 2021; Cisterna et al., 2022)	NoMaaS	Agent-based modelling for characterising the transport system *status quo*	X						
Berlin, Germany	MaaS	Agent-based modelling for the modal shift when introducing a MaaS scheme	X						
Smith et al. (Smith, Sochor, & Karlsson, 2018a), Smith and Sørensen (Smith & Sørensen, 2023) Sweden	Market-driven development	Surveys and interviews to identify roles in a MaaS ecosystem led by the private sector, no regulation from the public sector leads to the erosion of public transport and the emergence of private services		X			X	X	
	Public-controlled development	Surveys and interviews to identify roles in a MaaS ecosystem led by the public sector		X			X	X	
	Public-private development	Surveys and interviews to identify roles in a MaaS ecosystem where public and private sectors collaborate in the establishment and maintenance of such a scheme		X			X	X	
Enoch (Enoch, 2018) New Zealand	Mobility marketplace	Low development of the share economy and significant car ownership	X						
	Competitive commons	Share economy and reduced car ownership	X						
Enoch and Potter (Enoch & Potter, 2023) UK	Highly consolidated market, and highly consolidated services	At the local/regional level, the government oversees the service level and prioritises societal good. Yet, strong regulations may make it less financially attractive for transport service providers.	X		X		X	X	
	H. consolidated market and h. fragmented services	At the global level, this scenario considers large companies dominating the market. This increases the benefits for the users as providers are highly specialised in their sector, yet, innovation would be slowed as new there would be barriers for new players to enter the ecosystem.	X		X		X	X	
	H. fragmented market, and h. consolidated services	At the national scale, this scenario considers consortiums of small and large companies providing MaaS schemes. This improves innovation and stimulates competition, which would require competition regulations. A counter point is that users may be flooded with information and choosing the right	X		X		X	X	

(continued on next page)

Table 3 (*continued*)

Reference and context	Name	Description	Ecosystem integration	Organisational transition	Platform functionality	Incentives for users	Incentives for operators	Public governance	Cyber security
		membership could be confusing.							
	H. fragmented market, and h. fragmented services	This is the most common current model in urban areas, where many service providers offer a multitude of services and reach customers through third-party digital platforms. This scenario requires strong policy frameworks to ensure fair competition and adequate pricing.	X		X		X	X	
Enoch et al. (Enoch et al., 2020) New Zealand	Shared shuttles	Share economy in small and dense urban centres	X		X		X	X	
	Connected corridors	Automation and intelligent mobility reduce the time waiting and travel time	X		X		X	X	
	Mobility market	Car-based services dominate the market with little coverage of public transport	X		X		X	X	
	Personalised pods	Private and shared autonomous car-based services dominate the market	X		X		X	X	
Duan et al. (Duan et al., 2022) Australia	MaaS	A predictive model using Artificial Neural Networks to predict the purpose of MaaS user's travel (social, general, or work travel).		X					
Mitropoulos et al. (Mitropoulos et al., 2023) Athens, Greece	Multimodal work trip	Main users are travellers to/from central Athens from/to Northern Athens, moving around for work, education, and/or leisure purposes	X	X	X	X			
	MaaS for tourists	Main users are travellers arriving and departing from a central district of Athens for touristic purposes, using the principal transport hubs.	X	X	X	X			
	Interurban/ urban interfaces	Main users are travellers arriving and departing from a central district of Athens for touristic purposes such as work and shopping/leisure	X	X	X	X			
Vaddadi et al. (Vaddadi et al., 2020) And Zhao et al. (Zhao et al., 2020) Sweden	Private vehicle addiction	No supportive policies for MaaS development and public transport is not willing to share data	X		X		X	X	
	Private shared services	Supportive policies for MaaS development and public transport not willing to share data	X		X		X	X	
	'Trends win over policies'	No supportive policies for MaaS development, whilst public transport willing to share data	X		X		X	X	
	'MaaS is the new black'	Supportive policies for MaaS development and public transport willing to share data	X		X		X	X	
Wong et al. (Wong et al., 2020)	Modal displacement	Replacement of public transport with on-demand shared services	X					X	
	Modal convergence	All transport modes would converge to automated taxi-like services	X					X	

Both articles work under the same modelling framework and scenario characteristics.
Light-weighted and mechanically simple vehicles, automation allows for higher physical security and less structural protection than a conventional vehicle.

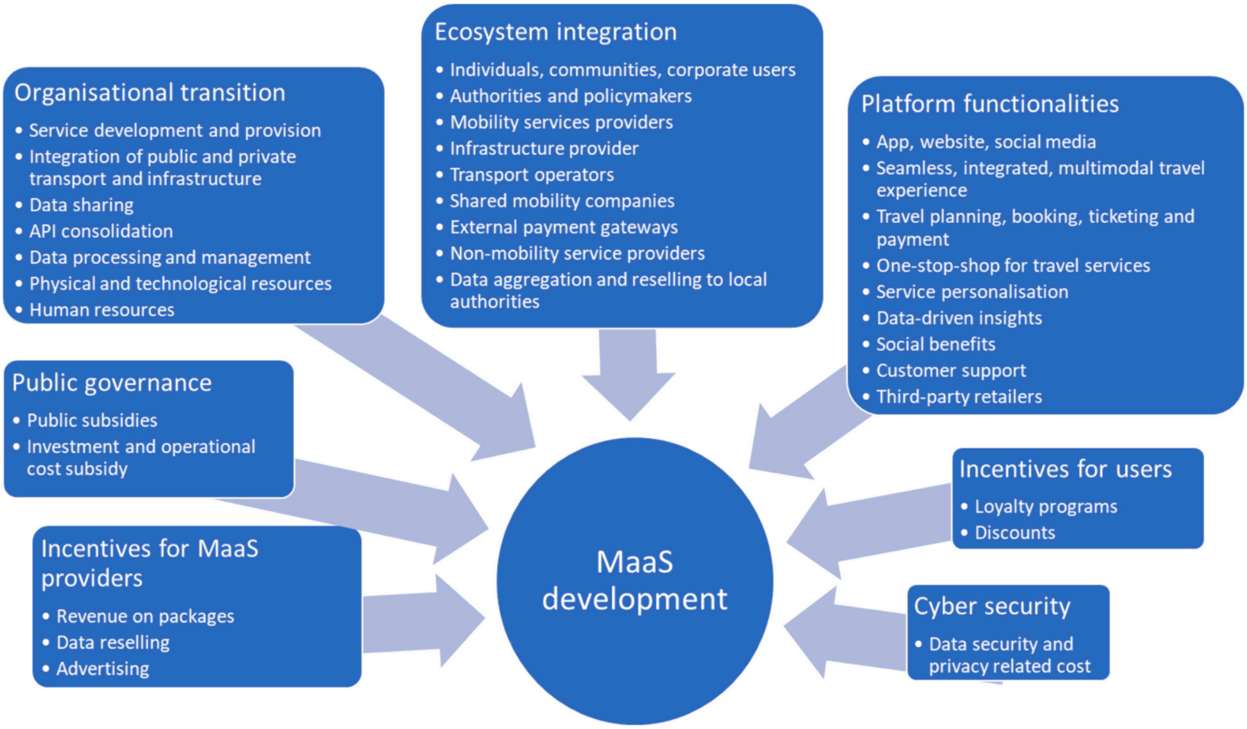

Fig. 6. A seven-dimensional matrix for MaaS development. (Adapted from Polydoropoulou et al. (Polydoropoulou et al., 2020) and Corazza and Carassiti (Corazza & Carassiti, 2021)).

data.

Hensher (Hensher, 2017) reported on specific policies such as subsidies for public transport tickets, and they mention that the question of how much should be subsidized is uncertain, especially given that the introduction of new services or transport modes may cannibalise some of the conventional transport services. Sakai (Sakai, 2019) noted that broad regulations such as the Intelligent Transport Systems Directive of the European Union (The European Parliament and the Council of the European, 2010) are in place to secure competitiveness and interconnectivity across organisations and countries. Although EU policies promote the integration of mobility services, it is up to each member state to establish local regulations. For instance, Finland has changed in driving license regulations to help the use of car-sharing services by allowing any vehicle to be used as a taxi (Smith, Sochor, & Sarasini, 2018b). However, as mentioned before, this could lead to a scenario where car-based services dominate public transport.

3.2.6. *Dimension 6: incentives for MaaS providers*

Despite an agreement on the need for incentives and subsidies to make the business model attractive for private actors (Hensher, 2017; Polydoropoulou et al., 2020; Smith, Sochor, & Karlsson, 2018a; Smith & Sørensen, 2023; Vaddadi et al., 2020; Zöschinger, 2019) in the early phases of development to cover the costs, what these incentives or subsidies may look like has been overlooked in the literature. Polydoropoulou et al. (Polydoropoulou et al., 2020) mentioned that concerns about the economic performance of public transport have led to global trends of transport deregulation. A common regulation change is to make reselling and bundling tickets of public transport tickets open to third-party actors [26,30,42]For instance, in the UK, more specifically in London, Stringer (Stringer, 2018) noted the need for regulations to protect public transport users when they use multiple transport modes in case of accidents or service disruptions. Stringer also conducted a review of the current legislation to identify the users' rights with particular consideration to the need for data-sharing policies.

3.2.7. *Dimension 7: cyber security*

Despite the extensive discussion on data sharing and integration, along with the need for policies to protect the users during multi-model journeys, there are only a few papers that mention cyber security risks that may arise from the development of integrated mobility services for both users and providers. Moreover, the reports of current MaaS schemes in Europe (MaaS4EU, MyCorrydor, Shift2MaaS and IP4MaaS) have not yet paid enough attention to this dimension, and focusing on the MaaS platform data privacy and personal data protection policies and mechanisms (Gkemou, 2018; Llp, 2024). Despite the UK government has published the *Mobility as a Service: code of practice*, there is no evidence that the MaaS literature or current schemes have accounted for similar threats to those from online banking. For instance, Kurmanova et al. (Kurmanova et al., 2021) report that within fraud and cyber attacks, phishing and malicious are prominent whit identify theft increasing over time. Therefore, one could argue that the emergence of cyber security risks experienced by the digitisation of traditional banking could be experienced in a larger magnitude by the integration of already-digitised transport services in a unique platform.

Pangbourne et al. (Pangbourne et al., 2018) noted that the central role of ICTs in MaaS points to potential significant disruptions through deliberate denial-of-service (DoS) cyber-attacks when access to transport is via the MaaS platform only. Corazza and Carassiti (Corazza & Carassiti, 2021) also highlighted the high technological dependency on MaaS, which raises the issue of data sharing and security standards. Moreover, such ICT dependency may also lead to social inequities and digital exclusion (Alyavina et al., 2022; Corazza & Carassiti, 2021).

3.3. Assessment of MaaS development scenarios

After developing the 7-D matrix, we assess its coverage in the selected 15 MaaS scenarios that comprise a variety of countries (i.e., Germany, Sweden and New Zealand) and scales (city and country size) (see Table 3). Among the 43 articles reviewed, cyber security is the most overlooked dimension, only two papers (Corazza & Carassiti, 2021; Pangbourne et al., 2020) paid attention to this. Yet, these authors do not elaborate on any scenarios or narratives of the development of MaaS or the potential impacts of cyber security risks on the other six dimensions. We then discuss potential cyber security risks that may emerge within each dimension in section 4.2.

Cisterna et al. (Cisterna et al., 2021) designed an agent-based model to explicitly characterise the spatial and temporal distribution of users for the city of Berlin. Then, the model evaluates the shift in the users' behaviours under two scenarios: **NoMaaS** (or **pay-as-you-go**) and **MaaS**. In the NoMaaS scenario, users pay for the used services throughout the day. In the MaaS scenario, there is a fixed price for the entire public transport network. The agents' decision-making is based on a utility function that considers their daily travel cost and benefits from activities, yet, this utility function does not include negative effects of external events, i.e., disruptions in the transport network or failure in the ICT infrastructure. Moreover, the scenarios only partially describe one of the seven dimensions presented in the previous section (ecosystem integration), which may limit the model to inform about the effects of the other dimensions on the agent's decision-making (and resulting utility function). Cisterna et al.'s results show that in the MaaS scenarios, the use of private cars remains at the same level, whilst walking or bike modes are shifted into public transport. Although public transport usage has doubled, the use of car-sharing also increased significantly. In their follow-up research, Cisterna et al. (Cisterna et al., 2022) expanded on the same modelling framework and scenarios by experimenting with variance in the subscription price, yet, this is still uniform across the population.

Similarly, Wong et al. (Wong et al., 2020) propose two scenarios for the development of cities' mobility services: **modal displacement** and **modal convergence**; disregarding rural areas or inter-city journeys. The former considers the replacement of public transport with on-demand shared services, thus, making efficient spatial and temporal use of the transport network. On the other hand, the modal convergence scenario assumes that all mobility services become autonomous taxi-like services. Although the authors recognise this is an extreme scenario, they analyse this as a potential pathway under the assumption of no or weak policies that protect the societal good. This scenario considers that other transport modes would converge to automated taxi-like services due to the need for pint-to-point services (buses), and the desire for low-cost service (cars and taxis). Although this modal convergence is expected to increase transport accessibility, it is not clear whether the increase in demand would cause traffic congestion or larger CO2 emissions.

Smith et al. (Smith, Sochor, & Karlsson, 2018a) and Smith and Sørensen (Smith & Sørensen, 2023) created three narratives that connect the transport sector to the users via a MaaS provider in Sweden. They defined two types of actors for MaaS providers: the integrator who liaises with transport providers, and the operators who create bundles and offers and deliver those to the users; then, each scenario corresponds to the nature of these actors (public or private).

Firstly, the **market-driven scenario** defines both actors as part of the private sector and there is no regulatory policy in place. In this scenario, MaaS focuses on maximising profit for operators and integrators, which may lead to more car-based services. Maybe not surprisingly, the focus on market aspects leads to opening ticket reselling to third parties (organisational transition) at subsidized prices (incentives for operators). The **public-controlled scenario** sets the possibility of creating a new organism/department that takes over the provider and operator roles (organisational transition), aiming to maximise the use of public transport and societal good (public governance). The third scenario, **public-private development**, incorporates the characteristics of the previous two scenarios that envision public-private development, where the integrator is from the public sector and the operator is a private actor. Consequently, in this scenario, the public sector facilitates and makes sure that MaaS looks after sustainable goals. Under these circumstances, the public sector absorbs some of the initial investments, making it more attractive for the operators (incentives for operators). Smith et al.'s three scenarios are not significantly different in terms of the other development elements we have highlighted before, hence, we refer interested readers to (Smith, Sochor, & Karlsson, 2018a; Smith & Sørensen, 2023) for further details.

Enoch (Enoch, 2018) investigated two MaaS scenarios for New Zealand: **mobility marketplace** and **competitive commons**. The main difference between these two scenarios is the population density. The second scenario assumes a higher population density, which drives a transport system with fewer private cars and more shared mobility. In further research, Enoch et al. (Enoch et al., 2020) develop other four MaaS scenarios defined by the variations of population density (high/low) and transport automation (partial or full automation). In **shared shuttles,** the high population density results in people travelling shorter distances from home to their daily activities. This increases the use of active travel (foot and bike) and shared minibuses/shuttle services in urban areas, this also makes shared services financially viable for areas with low-frequency demand. **Connected corridors** set a future where the high demand in urban areas is supplied by fully automated trains or rapid buses, whilst self-driving cars account for the last-mile part of the trip. Contrarily, the **mobility market** is the closest scenario to the current state of the transport system (in New Zealand), which considers low urban density and low penetration of automated vehicles. These characteristics make the market to be dominated by private cars and transport services focused on information services. **Personalised pods** assume a higher level or automation than the previous scenario and replace private cars with automated "pods" owned by mobility providers. The automation of the transport system allows to optimise travel time and reduce traffic congestion.

Vaddadi et al. (Vaddadi et al., 2020) developed four scenarios for the development of MaaS in Sweden, differentiated across two main dimensions: i) policies and regulations, and ii) openness of the public transport for integration. The first scenario, **private vehicle addiction**, assumes policies to be conservative and little supportive of MaaS where the public transport operators are not willing to collaborate on building-integrated mobility services. Although the services provided are limited, there is a relatively small reduction in car usage. The rise of the **private shared services** scenario considers proactive policies and regulations towards MaaS, but still, the public transport operators are not willing to collaborate. Building upon the previous scenario, the authors increase the share of car-based sharing services, which are considered the most flexible model. The next scenario, '**trends win over policies**', turns the tables considering not supportive policies towards MaaS but public transport willing to be integrated. The integration of public transport allows the emergence of MaaS to a limited degree, whilst shared services jointly seek profit. '**MaaS is the new black**' is the final scenario that assumes proactive policies and public transport operators' openness for collaboration, making MaaS available across urban and rural areas, and the application is fully functional. Vaddadi et al. reported the following indicators for each of the scenarios: car usage, car ownership, fossil fuel consumption and CO_2 emissions.

This section has shown that cyber security risks have been overlooked in the design and development of MaaS scenarios. Moreover, the number of articles for MaaS scenarios in the UK is limited to (Enoch & Potter, 2023) and outlining government initiatives to (Department for Transport, 2023). The former focuses on the consolidation of the market and services, whilst accounting for different geographical scales. The later recognises the key role of MaaS in providing sustainable rural mobility solutions.

Therefore, as part of our work, we organised an expert workshop with participation from the industry and academia to discuss and identify cyber security risks in the UK context.

3.4. Expert workshop results: cyber security risks in the context of the UK

A virtual expert workshop was held on December 7, 2021, as part of the research project “Mobility as a service: MAnaging Cybersecurity Risks across Consumers, Organisations and Sectors (MACRO)”, which is funded by the UK Engineering and Physical Sciences Research Council (EPSRC). The workshop comprised academic talks, two parallel breakout sessions and a panel discussion. Fig. 7 shows the share of academia, public and private sector attendees ($N = 15$), who were divided into two groups and asked to formulate different future MaaS scenarios in the UK context. Both groups were presented with the seven-dimensional matrix presented in Section 0 and encouraged to think of alternative dimensions or variables that may inform the further development of future MaaS ecosystems.

Group 1 suggested scenarios where a local authority (LA) takes the lead in the MaaS ecosystem to ensure that strategic objectives are not profit-driven. This scenario implies that users’ data is owned by the LA, whilst the MaaS providers work for the LA as sub-contractors. The number of users, i.e. the scale of the MaaS ecosystem, and a high enough travel frequency per person were deemed important for making the scheme commercially viable for private actors. In this scenario, the role of LA is assumed to provide accessibility and user support through the MaaS providers, including a call centre and an off-line booking system.

The group identified the importance of incentives to encourage a modal shift for more environment-friendly transport modalities such as walking, cycling and shared services. Such incentives are reported to include point-based discounts for services, discounts for local retailers, donations to charities, and credits purchased and distributed by employers to encourage their sustainable transport behaviours. Such incentives may become more effective if they are complemented via large marketing campaigns and digital schemes.

Group 2 were interested in a scenario where the private sector takes the lead in the MaaS ecosystem, whilst LAs may provide regulations to ensure societal good. In this scenario, transport system actors focus on having a strong public transport network with improved flexibility and coverage via emerging new technologies and other transport services (i.e., car sharing, micro-mobility). In this scenario, car-sharing services (for reducing the need for cars) and taxis (for faster response time) are included as they offer more flexibility. Other mobility innovations such as e-scooters can be integrated. This group noted that a mature MaaS ecosystem is one that contributes to users’ travel behavioural changes towards more sustainable choices.

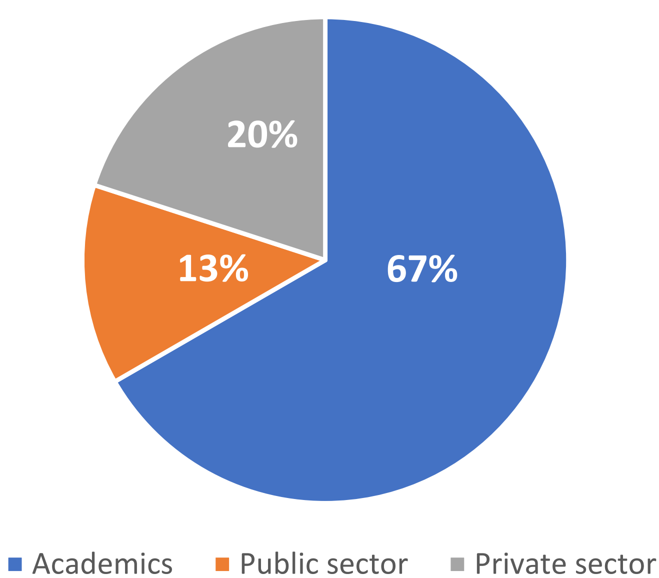

Fig. 7. Distribution of the workshop attendees’ sectors.

Because data exchanges play a central role in any MaaS ecosystem, both scenarios would require alignment of data application programming interfaces (APIs) and data security protocols in place, facilitating the data sharing among partners and stakeholders. Both groups agreed on the need for regulators to maintain connectivity privacy and transparency of algorithm and data usage.

Following the presentation of scenarios by each group, a plenary discussion took place. In cases where LAs own public transport, the participants noted that they should act as the MaaS operator. Yet in cases where public transport is owned by private actors, the participants noted the LA to work with the private sector in designing the MaaS ecosystem. This goes in line with Dulskaia Francesco (Dulskaia & Bellini, 2023) who pointed out that public-private partnerships, along with innovative business models, are key for the development of new mobility services.

As the regulatory framework is deemed important for ensuring sustainable goals, LAs are required to provide the regulatory framework. In particular, such a framework should ensure that the scale of the ecosystem covers as many users as possible to avoid social inequities and digital exclusion. In the context of enhancing accessibility and inclusiveness, reaching areas with low latency of service may incur additional costs for the transport suppliers. Because users may have different objectives (i.e., local travel vs intercity commuting), the ecosystem shall also account for the services in an “extended coverage”, even if these are not included explicitly in the platform. It was also suggested that data should be shared at the national level, even if different MaaS ecosystems cover only local areas.

It was noted that the interaction of the MaaS boundary with adjacent areas requires further consideration as there might be users who travel from outside their local MaaS ecosystem. A suggestion was made to consider the rest of the transport network more holistically. The potential of micro-mobility for first- and last-mile to increase the flexibility and coverage of the service, as well as inter-county transport, was highlighted. Both groups noted the relevance of incentives, whether for promoting a more modal shift or value creation for users and organisations. However, no further discussion took place than the possibility of using point-based incentives for walking, cycling and shared services.

To inform the discussions on **cyber security risk management**, three academic presentations were made, followed by a plenary discussion. Three key themes were identified: i) data sharing and emerging cyber security risks, ii) costs of data sharing and algorithm ownership, and iii) data-sharing and privacy principles. The first point considers the current situation where data is still segmented and held by each of the transport providers, resulting in its full value being unknown and under-exploited. It was pointed out that for public and private organisations to cooperate, those originations must understand how data sharing creates value for users and organisations, i.e., expanding the customer base. Moreover, these organisations must acknowledge that new cyber security risks will emerge due to increased data-sharing activities.

Besides the benefits that data sharing could bring to the MaaS actors, a recurrent concern was the potential (additional) costs of data sharing. In this context, different actors may face different barriers due to their different capabilities for managing data-sharing activities (i.e., large organisations vs start-ups). Participants also mentioned the need to establish who the data and algorithm owner (including understanding and managing the network of data flows) will be.

To address and manage data flows between different actors, a framework like a code of conduct can be used. Such a framework can define fundamental data-sharing principles for MaaS ecosystems and include a template for data privacy impact assessment (DPIA) exercises for public and private actors. The proposed system architecture for the MaaS provider will allow only MaaS partners to see all data, e.g., in the LA-led scenario, even the LA will not have full visibility of data (instead, a back-office platform not controlled by the LA will see all data and do the necessary data integration) and the MaaS operators being data processors on behalf of the LA. Such a system may have a frontend and different dashboards for different groups of users to do data analysis. From a user's perspective, their data goes into the MaaS platform via a privacy-preserving endpoint aggregation (PPEA) module, meaning that actual individual values are not shared with the MaaS operators.

4. Further discussion and research agenda

Section 3.2 presents a seven-dimensional matrix that groups narratives, classifications, barriers and drivers, and business models' building blocks. The matrix has been used to assess the coverage of this 7-D in selected MaaS scenarios reported in the literature, showing the current state of the scenario's design and MaaS demonstrations. The matrix can help map the maturity of MaaS projects and required changes in local and regional transport ecosystems, as well as create more robust scenarios that consider cyber security extensively. The rest of this section discusses (i) the key findings from the literature on MaaS development scenarios, (ii) potential cyber security risks that may emerge across the other six dimensions, and (iii) avenues for future research to improve the modelling of MaaS ecosystems to ensure their cyber security.

4.1. Importance of cyber security risks

Our results suggest that **ecosystem integration, functionality,** and **organisational transition** categories have been widely studied in the literature. On the other hand, **incentives for users**, **incentives for MaaS providers**, **public governance** and **cyber security** are areas that require further research. Then, Section 3.4 summarises the insights from an expert workshop on the emergence and relevance of cyber security risks for the development of MaaS in the UK. Whilst we note the exploratory nature of the findings from the expert workshop (due to the small size of participants), we have unpacked the importance of the governance model of MaaS ecosystems which is confirmed by limited consideration of the **public governance** dimension in MaaS scenarios (see Table 3). In the UK, public policies have reduced the funding for public transport by ~40%, and recently public transport has exercised a decrease in usage due to COVID-19 and flexible working arrangements (Local Government Association, 2021). Because some services are not profitable, transport providers have withdrawn those services with a lower demand and longer distances (usually in rural areas), which may lead to social inequities (Local Government Association, 2021). Moreover, as described in some of the MaaS scenarios, the erosion of public transport leads to the emergence of car-based mobility services and the reduction of social benefits. Under these circumstances, one could argue that the **incentives for users** and **incentives for MaaS providers** may help with addressing the lack of public funding. For users, the adoption of MaaS may be hindered by the state of the vehicles which cannot be modernised because the transport supplier cannot afford to renovate or switch to low-emission vehicles (i.e., electric or hydrogen cars) (Local Government Association, 2021). For MaaS providers, this suggests that their value proposition should allow the transport suppliers to earn enough profit without putting extra charges on the users. Some of the workshop attendees mentioned that at least a county-level[4] scheme is necessary for making this attractive and financially viable for the MaaS provider. In the UK, this aligns with McTigue, Monios and Rye (McTigue et al., 2018) who mentioned that Transport Authorities and Local Transport Strategies in Scotland are not required to monitor the performance of local transport, and they may lack staff, funding and time to implement public transport policy (McTigue et al., 2018). On the other hand, in England, the Passenger Transport Executive are local government bodies that establish the level of service provided by rail mode and service provision by bus mode. They recognise that rail should be prioritised because the larger operational distances require more capital (Docherty, 2000). However, there is little discussion on the volume (total demand) required to make this financially attractive for the MaaS supplier nor the coverage of the scheme (area of service). Thus, whilst the **ecosystem integration** dimension focuses on data sharing, the **organisational transition** dimension should consider how to address the lack of staff and expertise MaaS-relevant public bodies possess.

Through the sessions of the expert workshop, it was also noted that potential value creation for the customers will emerge from new ventures and other non-transport services that may be included in the platform (**organisational transition** and **incentives for users**). On the other hand, workshop discussions highlighted the differences between the leading bodies in two different MaaS scenarios. In these scenarios, the ecosystem may be led by the public sector where the MaaS provider works as sub-contractors, or where the private sector leads the ecosystem and the public sector acts as regulators to ensure the societal benefits. Interestingly, the Local Government Association (LGA) in the UK reported that successful implementations of multi-modal transport schemes are often the results of private initiatives rather than public projects (Local Government Association, 2021). This may be partly because of the lack of public policies on public transport, as the result of focusing on economic benefits and overlooking social and environmental benefits (Local Government Association, 2021). On the other hand, private initiatives such as Corporate Mobility as a Service (CMaaS), studied by Zhao et al. (Zhao et al., 2020), face design barriers to integrate with public transport due to taxation issues, not enough demand to be profitable, and inability to provide sustainable solutions. Even for a private MaaS, the authors mention that public policies and incentives are required to promote users' behavioural change and companies to take part in MaaS ecosystems.

The discussion highlighted that data sharing is the main driver for the emergence of cyber security risks. This raised the questions of who the data and algorithm owner(s) should be and what degree of visibility each actor may hold for what type of data. Although the emerging literature focuses on data sharing implications and data privacy regulations, it has been highlighted that cyber-physical systems (such as the MaaS ecosystems) are vulnerable to multiple vulnerabilities and threats (Pundir et al., 2022). Pundir et al. (Pundir et al., 2022) classify these into (i) network vulnerabilities, (ii) platform vulnerabilities, and (iii) management vulnerabilities. The first exploits vulnerabilities at the physical level (wired and wireless communication devices) and may lead to breaches in data or denial-of services. Second treat.

Yet, to the best of our knowledge, there is no research on how these may impact the MaaS ecosystems, nor for conceptual models or study cases. Furthermore, we argue that cyber security aspects of MaaS development are not an independent dimension, but transcends through the other dimensions. In other words, cyber security has implications on the characteristics of the other six dimensions that make up the MaaS ecosystem. For example, cyber security risks could emerge from the **ecosystem integration** dimension in the form of uneven cyber security capabilities that could endanger the whole ecosystem; or from the **incentives for users** dimension for digital exclusion that could emerge from limited access to smart devices (e.g., smart phones, tablets, and smart watches) to earn benefits (Schikofsky et al., 2020). Therefore, the rest of the section discusses how cyber security applies to all other six dimensions and how considering cyber security risks better can help improve the modelling and simulation of MaaS ecosystems, therefore providing better tools to researchers, practitioners and policy makers who are interested in MaaS.

[4] Counties are administrative and geographical areas in the UK, these correspond to the European nomenclature of territorial units for statistics level 2 (NUTS2). In general, counties group local authorities (NUTS1), with an average population around 1 million; except for Greater London with a population around 9 million (Office for National Statistics O, 2012).

4.2. Identifying cyber security risks in MaaS scenarios

4.2.1. Dimension 1: MaaS ecosystem integration

Despite the extensive number of insights about data integration, cyber security risks have not been mapped into the potential MaaS business models nor considered as a factor for the MaaS scenarios. This disregard occurs across different MaaS levels of integration, meaning that cyber security risks have not been considered for schemes with "Integration of services", nor for MaaS solutions with level of integration (those with integration of information, booking and payment but no multimodal services). This means that the integration of individual services currently facing cyber security risks has not been accounted for in the literature scenarios or model business. For instance, Dulskaia and Bellini (Dulskaia & Bellini, 2023) present the BMC for taxi e-hailing, shared e-scooters, car-sharing, and bike-sharing with no regard for cyber security risks.

The cyber security subject is only reflected in one prototype of the business model (Polydoropoulou et al., 2020), but there is no discussion on how transport services' provision might be shaped by data security measures or practices. Moreover, cyber security risks are not only relevant for the ICT and transport infrastructure but also for transport users. Given that the development of MaaS requires the integration of data and services into a single platform, the level of integration does not only reflect the maturity of the system (Corazza & Carassiti, 2021) but also may reflect the potential impact on the system in the case of service disruption (Pangbourne et al., 2020). In other words, these scenarios that suggest a higher level of integration might as well assume a higher potential of disruptions in the transport system in the case of a cyber attack. Given that the degree of data sharing required (or defined in each scenario) is contingent upon cooperation among the transport operators and technical components (ICTs), regulatory frameworks are also needed (Corazza & Carassiti, 2021), which is discussed later.

To give a concrete example of cyber security risks relevant to this dimension, one can consider the over-aggregation of personal data of transport users due to the integration of the whole ecosystem where all transport operators share data about transport users with the MaaS provider. This can lead to privacy concerns from transport users' perspective, and therefore some technical solutions are required to address such concerns. One possible solution is federated learning (Yin et al., 2021), which allows multiple transport operators to work together without sharing their local data. Another example is the enlarged attack surface on participating systems, where malicious parties (including transport operators and users) now may be able to deliberately inject false data into the MaaS system for their benefit (Ahmed & Pathan, 2020).

4.2.2. Dimension 2: platform functionality

Three wide digital functions, booking, payment and real-time information, were considered by Enoch (Enoch, 2018). These three functions may require external gateways to provide services to the user, for instance, the user's payment information for buying a ticket goes through a gateway to a bank supplier and then to a transport provider. Moreover, as new services emerge within the MaaS ecosystem, its scope would extend to non-transport services such as parking or EV charging station payments (Stringer, 2018). Therefore, with more services and more gateways involved in a MaaS system, more cyber security risks are likely to emerge. The increase in the number of services also implies more data sources that need to be integrated into a single platform and provided to the user in real-time. It has been noted that users hesitate to change to active travel modes (walking, cycling, etc.) if there is no routing information for those. Then, arguably, this could be extended to other types of transport modes, moreover, a reliable information system is required for the users to plan their journeys.

One example area of cyber security risks for this dimension relates to the fact that the MaaS concept relies on the concept of personalisation and it has been noted that customers respond substantially to subscriptions (Corazza & Carassiti, 2021). This requires collecting the user's personal data and travelling patterns to be processed and used for marketing purposes, which raises two potential risks: micro-targeting and digital exclusion. The first means malicious or adversarial activity from organisations or individuals to identify or classify targeted transport users throughout their digital footprints, intending of targeting them with specific advertisements or information. The second does not look at the MaaS users, instead, it focuses on those with no access or limited access to the platform. This may lead to social inequities, as subscriptions and potentially cheaper offers may not be available for traditional payment methods (Pangbourne et al., 2018; Schikofsky et al., 2020). For instance, Alonso-González et al. (Alonso-González et al., 2020) report that potential Dutch MaaS users with conservative and opposing attitudes towards new mobility services do not own a smart phone and/or a mobile internet subscription (29% and 22%; 79% and 43% respectively).[5]

4.2.3. Dimension 3: organisational transition

The question of who the MaaS provider should be has been raised, whether this is public, private or a mix of both, there are still other roles to be covered and changes to business models to be made. Furthermore, because the MaaS ecosystem is an evolving system with a continuously increasing number of actors (Corazza & Carassiti, 2021) (start-ups or innovative businesses (Smith, Sochor, & Sarasini, 2018b)), business models and relationships will be in continuous evolution. This means that data transactions will be made through (external) gateways communicating an increasing number of organisations with different cyber security capabilities. Therefore, there are potential weak spots in the chain of communication that could be exploited to compromise the whole ecosystem, leading to so-called supply chain attacks (Urciuoli et al., 2013). Therefore, there is a need for cyber security standards and regulations to ensure the security and privacy of users' digital data. Moreover, the MaaS ecosystems may also be subject to differences in cross-border regulations which is critical for the transport sector when moving passengers or freight from one country to another (Cottrill, 2020).

In the UK, MaaS ecosystems such as the one in South England or Great Manchester and Leicestershire have emerged from different approaches. The former is a Maas ecosystem known as The Solent Region (Solent Future Transport Zone, 2024), which provides multicity multimodal travel to Southampton City Council, Portsmouth City Council, Isle of Wight Council, and Hampshire County Council. The transport services can be accessed through the Breeze app developed in collaboration between the University of Southampton and Transport (Solent Transport, 2024). On the other hand, Great Manchester and Leicestershire have relied on the use of a third-party actor which provides a white-label platform to the local government. The industry of white-label solutions has emerged as the result of new software business models, offering public bodies *plug-and-play* MaaS solutions (Caballini et al., 2023). This software is a digital product that can be rebranded by another organisation, for instance, Wunder Mobility (*Wunder Mobility: market-leading software provider for shared mobility operators*, 2024), MoveYou (*Seamlessly accessible - MoveYou*, 2024), FlowBird (*Flowbird - Urban intelligence*, 2024), Trafi (*Trafi: Vilnius app*, 2024), and SKEDGO (*Leicester City Council*, 2024) provide unbranded platforms for MaaS, the latter provides journey planners to the Greater Manchester and Leicestershire transport authorities (individually). Similar to Smith et al.'s (Smith, Sochor, & Karlsson, 2018a) and Smith and Sørensen (Smith & Sørensen, 2023) scenarios describe a scenario where the public and private sector cooperate, with the public sector liaising with the transport providers whilst the private sector develops the front (platform) and back-end

[5] By 2017, the Netherlands had a larger share of individuals who access internet via a smartphone than the UK (~69% vs ~65%) (European Commission, 2024).

(data processing) (Dulskaia & Bellini, 2023; Hodson et al., 2023; Schneider & Koska, 2023).

The benefits of such white-label solutions include increasing the public acceptance of the MaaS ecosystem because the service is perceived as part of the public offering, as well as making MaaS more attractive for private actors (Schneider & Koska, 2023). Moreover, this structure helps local authorities to have more control over the MaaS ecosystem (Hodson et al., 2023). Schneider and Koska (Schneider & Koska, 2023) also mention that the white-label application can help scale the coverage of MaaS in a cross-municipalities ecosystem by linking local ecosystems, avoiding the need for a new platform for the larger area.

Nevertheless, some of the platform functionalities (Dimension 2) may be limited and extra features will come with a cost (Schneider & Koska, 2023). Despite the software providers having a clear privacy and data protection policy, some of the extra features can include cyber security add-ons (Adjust, 2024).

4.2.4. Dimension 4: incentives for users

While the role of incentives to help change the users' travel behaviours is noted (Corazza & Carassiti, 2021; Hensher, 2017; Pangbourne et al., 2018; Smith, Sochor, & Sarasini, 2018b; Stringer, 2018; Zhao et al., 2020; Zöschinger, 2019), they could also be used to prompt better cyber security behaviours and reduce associated risks. In the public domain, Coventry et al. (Coventry et al., 2014) note that from the emerging research on cyber security, the factors that drive behavioural change can be classified into environmental, social and personal factors. These include inbuilt cyber security features, incentives (rewards or sanctions), social norms, understanding of cyber security and personal perceptions and attitudes. In particular, they pointed out that, if costs (e.g., penalties or financial sanctions) are lower than benefits (e.g., free products, discounts, vouchers), then users can demonstrate unsafe cyber security practices and behaviours (e.g., disclosing personal information); some of these factors have an objective value and others a subjective. Arguably, these insights could be transferred from the cyber security domain to the mobility domain. Therefore, both, the modelling of behavioural change towards cyber security and the analysis for incentivising travel mode shift through MaaS adoption should account for objectives and subjective values. Additionally, environmental benefits should be considered to justify the government incentives, otherwise, the business model does not offset the operational costs (Ho, 2022).

From a different perspective, one could pressure the presence of malicious users, those who may exploit the MaaS ecosystem's benefits or incentives seeking financial gain (Trowbridge et al., 2018). For instance, malicious users could use algorithms to obtain free mobility services, accumulate extra incentives or steal benefits from other users, resulting in incentives/benefits becoming a cyber-attack vector. Arguably, other dimensions could also be targeted by these malicious users. For instance, false information could be fed into the ecosystem and affect the information system used to inform other users (i.e. traffic and road conditions, availability of services).

4.2.5. Dimension 5: public governance

Some of these activities should also be reinforced by regulations that look after societal good, acknowledging the complex evolution and emergence of data streams (Cottrill, 2020). For instance, mechanisms are to be in place to prevent data monopolies and the ecosystem aims primarily to optimise the public transport system and avoid its cannibalisation by car-based services. Another example is to define more transport-specific regulatory guidelines on the data protection law such as the GDPR in the EU and the UK to offer more protection for user privacy, which can require and nudge business actors in a MaaS ecosystem to consider the security and privacy of users' data more seriously and make their data protection practices more transparent to users. This could in turn encourage more users to adopt MaaS, including those more environment-friendly travel modes. Such guidelines should be jointly defined by the data protection authority (e.g., the Information Commissioner's Office in the UK), the public body in charge of public transport (e.g., the Department for Transport in the UK), and local authorities leading a MaaS system or supporting a MaaS system led the private sector.

4.2.6. Dimension 6: incentives for MaaS providers

The MaaS initial cost and value creation model may represent a barrier for public or private actors to step forward as MaaS providers. There is a unanimous agreement on the need for financial incentives and subsidies to make MaaS economically viable for the private sector (Hensher, 2017; Polydoropoulou et al., 2020; Smith, Sochor, & Karlsson, 2018a; Smith & Sørensen, 2023; Vaddadi et al., 2020; Zöschinger, 2019). Some of these incentives may also be extended to other actors within the ecosystem to act as a catalyst for their willingness to cooperate and share data. Moreover, financial aid in the form of competitive grants and interest-free loans can be offered by public bodies to help MaaS-relevant organisations bring their cyber security capabilities to the level required for securing the whole ecosystem. Yet another perspective is how to incentivise the MaaS supplier to promote better cyber security practices and behaviours among users and share insights on the weak spot with the rest of the ecosystem. MaaS suppliers could be incentivised by financial rewards or recognitions from public bodies, industry associations and consumer bodies to encourage them to be more actively participating in such cyber security awareness activities.

4.3. Improving modelling of MaaS ecosystems

Following the evidence on the importance and dependence of the other six dimensions to cyber security in enabling the maturity of the MaaS ecosystem, we then assessed the robustness of MaaS models to represent cyber security risks. Given the individual nature of the decision-making related to the MaaS development (travel modal shift and cyber security behaviour), this section focuses on improving the Agent-based model (ABM) The ABM is a microscopic approach that explicitly characteries spatio-temporal distribution of single users with diverse purposes and preferences (Corazza & Carassiti, 2021).

Our review of MaaS scenarios shows that some of these have informed about the changes in users' preference towards different transport modes (Cisterna et al., 2021; Hensher, 2017; Matyas & Kamargianni, 2019), whilst others describe some elements of the MaaS ecosystem, focusing on the behaviours and roles of some actors of the transport system (Enoch et al., 2020; Jittrapirom et al., 2017; Smith, Sochor, & Sarasini, 2018b). Yet, current scenarios have overlooked the complexity of the MaaS development, resulting in MaaS models that simplify the characterisation of the MaaS ecosystem by only including a few dimensions in their design. For example, simple scenarios such as the Cisterna et al. model (Cisterna et al., 2021) and Alonso-González et al.'s. (Alonso-González et al., 2020) are useful to understand general shifts of transport mode in the presence of a MaaS scheme or extreme pathways, respectively. Yet, these fail to inform on specific areas of MaaS development such as the effect of incentives for users or the required maturity level of the ecosystem (**ecosystem integration**) to maximise the societal good. Moreover, both studies consider only citizens within an area/city, thus, the results disregard those individuals who travel into and out of the area/city, potentially, travelling into areas with lower demand and higher prices. Bushell et al. (Bushell et al., 2022) also mention that users who travel to other cities are more likely to spend more time pondering modal choices, thus, they need to have seamless and consistent familiarity with the mobility services that MaaS provides.

Another limitation of Cisterna et al.'s model is the homogeneous characterisation of the population. There are two implications to this, first, given the subjective values of preferences and beliefs, it may be difficult to calculate a value for perceived environmental or social benefits. Such models focus on the modal shift using rational choice modelling, which ignores individual preferences or subjective benefits. Thus, hybrid modelling approaches are required to account for the mode preferences and cyber security risks perception. The second limitation are that these values may vary across the population given the differences in socioeconomic characteristics (Amblard & Quattrociocchi, 2018; Bale et al., 2015; Farmer & Foley, 2009; van Duinen et al., 2016). In further research, Cisterna et al. (Cisterna et al., 2022) expanded on the same modelling framework and scenarios by experimenting with different subscription prices, yet, these are kept uniform across the population. Therefore, models like Cisterna et al. could benefit from including different utility functions based on the individual's preferences and benefits other than financial ones to introduce the cost and benefits of cyber security risks and data sharing behaviour.

There are examples in the transport domain that highlight the impact of users' technological understanding and perception on the adoption of mobility innovation. For instance, Struben and Sterman (Struben & Sterman, 2008) pointed out that a specific user's understanding and perception of electric vehicles can be a barrier for that person to adopt MaaS. They developed an agent-based model that integrates the user's *willingness to try* a new technology into the agent's utility function. They also proposed to integrate the evolution of such factors over time, as it is noted that reservations for adoption diminish through experience and *word of mouth*. In another related work, van Schaik et al. (van Schaik et al., 2017) pointed out that a relevant factor for risk management is the user's perception of risk. Therefore, we argue that modelling the development of MaaS requires including the evolution of the users' perception of cyber security risks into the user's utility function. This also implies the inclusion of a temporal variable into the model to produce insights into how the pace of integration changes in response to perceptions and attitudes towards cyber security risks.

The articles that focus on possible roles and attitudes of the public and private sectors highlight some pitfalls in the development of MaaS under certain circumstances, for instance, the propensity of the private sector to focus on maximising profit and car-based services (Vaddadi et al., 2020). However, there is no notice of how cyber security risks may lead to situations where society may face unintended consequences such as bias, exclusion, etc. (Butler et al., 2021). We argue that malicious algorithms could be used by both malicious or dishonest users and participating organisations for their own illegitimate benefits, e.g., for a transport supplier to promote services or packages that favour itself but not the users, and for a malicious user or external actor (who can be registered as a legitimate user) to disrupt the whole MaaS system. Additionally, a proposal to review the regulations to protect public transport users (Stringer, 2018) raised the question of what would be the role of the public and private sectors in safeguarding the security and privacy of users' data.

Finally but not least, considering cyber security risks in a MaaS model will require modelling other important aspects, including but not limited to the technical working of different cyber attacks, relevant behaviours of attackers, responses of victims and MaaS stakeholders, data flows an attack would lead to, and also interactions with relevant regulatory frameworks such as data protection and privacy laws. It is expected that including these factors in new modelling approaches provides a deeper understanding of the MaaS development.

4.4. Research limitations

It is acknowledged that the review methodology uses a strict list of keywords and that the screening of studies by a single reviewer might have had an effect on the results [Whitaker]. This may imply that relevant studies could be missed if the articles are not classified under these keywords, nevertheless, the snowballing criteria improves the reliability of the review and allows a systematic update of the emerging literature into the analysis [Greenhalgh] [Sayers]. Additionally, the reader must consider that our findings are based on peer-reviewed and publicly available material that may not have been peer-reviewed, disregarding publicly unavailable company reports or material that could contain Intellectual Property (i.e. current business models, technical and operational reports). We also acknowledge that our review might present an imbalanced number of studies across qualitative and quantitative approaches, and it is limited to publicly available reports on the current MaaS ecosystems.

5. Conclusions and recommendations

Finally, we summarise our findings reported in this paper and make recommendations for the following research avenues:

- Our work reported in this paper shows the disconnect between the two strands of literature: the studies on factors driving the development of MaaS and those on narratives of MaaS scenarios. This gap results in the inability to inform on the required strategies and policies to move from the current state of the transport system towards the desired MaaS ecosystem. Our 7-D matrix could be used not only to assess the maturity level of the current systems but also its potential to help design more robust models and scenarios. For instance, those models with rather simple scenarios reported in the literature could integrate the missing dimensions to inform policymakers on the potential pathways of MaaS development more realistically.
- Our results also highlight that both literature strands have largely overlooked the cyber security aspect of the development of MaaS. Moreover, by impacting the other six dimensions we present their vulnerability to cyber security risks. Yet, a more comprehensive survey on related cyber security risks is necessary, covering socio-technical aspects. Such future work can also cover how such cyber security risks can be considered for modelling MaaS ecosystems.
- We have discussed how cyber security risks may emerge in areas other than the ICTs and transport infrastructure. For the integrity of users' digital data, research is required for a deeper understanding of the users' response to incentives that prompt safer cyber security behaviours, and what role the public and private sectors may play in deploying these strategies. A microscopic approach such as agent-based modelling may allow characterising the users' behavioural change when incentives are introduced. Moreover, it could be assessed to what degree different types of incentives help to reduce cyber security risks for what type of organisations or individuals. Further research is also needed on the legislative framework for transport services to inform the design of regulations that promote data sharing and the protection of the integrity of users' digital data. This could be addressed by engaging with the MaaS stakeholders, both users and organisations and understanding their motivations and data sharing preferences and capabilities to identify how interventions and incentives may enable the cyber security of MaaS ecosystems.

Financial disclosure

This work was supported by the Engineering and Physical Sciences Research Council, part of the UK Research and Innovation (UKR), under the grant number EP/V039164/1.

We would like to thank all participants of the expert workshop, who provided great insights into our work and some of the results reported in this paper.

CRediT authorship contribution statement

Ali Alderete Peralta: Conceptualization, Formal analysis, Investigation, Methodology, Writing – original draft. **Nazmiye Balta-Ozkan:** Formal analysis, Methodology, Writing – review & editing. **Shujun Li:** Validation, Writing – review & editing.

Declaration of competing interest

We wish to confirm that there are no known conflicts of interest associated with this publication and there has been no significant financial support for this work that could have influenced its outcome.

Data availability

Data sharing does not apply to this article as no new data were created or analysed in this study.

Acknowledgements

This work was supported by the Engineering and Physical Sciences Research Council, part of the UK Research and Innovation (UKR), under the grant number EP/V039164/1.

We would like to thank all participants of the expert workshop, who provided great insights into our work and some of the results reported in this paper.

Appendix A. Appendix

Table 4
Seven-dimensional classification of the MaaS ecosystem building blocks and their consideration in MaaS literature.

Dimension	BMC's factor	BMC's building block	Strands of MaaS literature	
			MaaS scenarios	Development factors
Organisational transition	Service development and provision	Key activities	(Enoch et al., 2020; Smith, Sochor, & Karlsson, 2018a)	(Corazza & Carassiti, 2021; Mulley, 2017; Pangbourne et al., 2020; Polydoropoulou et al., 2020; Smith, Sochor, & Sarasini, 2018b; Stringer, 2018; Vitkauskaite & Vaiciukynaite, 2020; Wong et al., 2020; Zhao et al., 2020)
	Integration of public and private transport and infrastructure	Value proposition	(Enoch, 2018; Enoch et al., 2020; Smith, Sochor, & Karlsson, 2018a; Vaddadi et al., 2020)	(Corazza & Carassiti, 2021; Pangbourne et al., 2020; Polydoropoulou et al., 2020; Smith, Sochor, & Sarasini, 2018b; Stringer, 2018; Tinnilä, 2016; Wong et al., 2020; Zhao et al., 2020)
	Data sharing	Key activities	(Corazza & Carassiti, 2021; Enoch et al., 2020; Vaddadi et al., 2020)	(Corazza & Carassiti, 2021; Pangbourne et al., 2020; Stringer, 2018; Wong et al., 2020)
	API consolidation	Key activities	(Enoch, 2018; Smith, Sochor, & Karlsson, 2018a; Vaddadi et al., 2020)	(Corazza & Carassiti, 2021; Kamargianni et al., 2016; Pangbourne et al., 2020; Polydoropoulou et al., 2020; Smith, Sochor, & Karlsson, 2018a; Stringer, 2018; Vitkauskaite & Vaiciukynaite, 2020)
	Data processing and management	Key activity	(Enoch, 2018; Smith, Sochor, & Karlsson, 2018a)	(Corazza & Carassiti, 2021; Polydoropoulou et al., 2020; Smith, Sochor, & Sarasini, 2018b)
	Physical and technological resources	Key Resources	(Enoch, 2018; Enoch et al., 2020; Vaddadi et al., 2020)	(Corazza & Carassiti, 2021; Pangbourne et al., 2020; Polydoropoulou et al., 2020; Stringer, 2018; Vitkauskaite & Vaiciukynaite, 2020; Wong et al., 2020; Zhao et al., 2020)
	Human resources	Key Resources		(Polydoropoulou et al., 2020; Zhao et al., 2020)
Ecosystem integration	Individuals, communities, corporate users	Customer Segments	(Enoch, 2018; Enoch et al., 2020)	(Corazza & Carassiti, 2021; Kamargianni et al., 2016; Pangbourne et al., 2020; Polydoropoulou et al., 2020; Stringer, 2018; Vitkauskaite & Vaiciukynaite, 2020; Wong et al., 2020; Zhao et al., 2020)
	Authorities and policymakers	Key Partners	(Enoch, 2018; Enoch et al., 2020; Smith, Sochor, & Karlsson, 2018a; Vaddadi et al., 2020)	(Corazza & Carassiti, 2021; Kamargianni et al., 2016; Pangbourne et al., 2020; Polydoropoulou et al., 2020; Smith, Sochor, & Sarasini, 2018b; Stringer, 2018; Vitkauskaite & Vaiciukynaite, 2020; Wong et al., 2020; Zhao et al., 2020)
	Mobility services providers	Key Partners	(Enoch, 2018; Enoch et al., 2020; Smith, Sochor, & Karlsson, 2018a; Vaddadi et al., 2020)	(Corazza & Carassiti, 2021; Kamargianni et al., 2016; Pangbourne et al., 2020; Polydoropoulou et al., 2020; Smith, Sochor, & Karlsson, 2018a; Stringer, 2018; Tinnilä, 2016; Vitkauskaite & Vaiciukynaite, 2020; Wong et al., 2020; Zhao et al., 2020)
	Infrastructure provider	Key Partners	(Enoch, 2018; Enoch et al., 2020; Vaddadi et al., 2020)	(Corazza & Carassiti, 2021; Kamargianni et al., 2016; Polydoropoulou et al., 2020; Vitkauskaite & Vaiciukynaite, 2020; Wong et al., 2020)
	Transport operators	Customer Segments	(Enoch, 2018; Enoch et al., 2020; Smith, Sochor, & Karlsson, 2018a; Vaddadi et al., 2020)	(Corazza & Carassiti, 2021; Kamargianni et al., 2016; Pangbourne et al., 2020; Polydoropoulou et al., 2020; Smith, Sochor, & Karlsson, 2018a; Stringer, 2018; Tinnilä, 2016; Vitkauskaite & Vaiciukynaite, 2020; Wong et al., 2020; Zhao et al., 2020)
	Shared mobility companies	Key Partners	(Enoch, 2018; Enoch et al., 2020; Vaddadi et al., 2020)	(Corazza & Carassiti, 2021; Mulley, 2017; Pangbourne et al., 2020; Polydoropoulou et al., 2020; Stringer, 2018; Vitkauskaite & Vaiciukynaite, 2020; Wong et al., 2020; Zhao et al., 2020)
	External payment gateways	Key Partners	(Vaddadi et al., 2020)	(Corazza & Carassiti, 2021; Kamargianni et al., 2016; Pangbourne et al., 2020; Polydoropoulou et al., 2020; Stringer, 2018; Wong et al., 2020; Zhao et al., 2020)
	Non-mobility service providers	Key Partners	(Vaddadi et al., 2020)	(Corazza & Carassiti, 2021; Kamargianni et al., 2016; Polydoropoulou et al., 2020; Tinnilä, 2016; Wong et al., 2020)
	Data aggregation and reselling to	Revenue Streams	(Vaddadi et al., 2020)	(Corazza & Carassiti, 2021; Stringer, 2018)
	Local authorities	Key Partners	(Enoch, 2018; Enoch et al., 2020; Smith, Sochor, & Karlsson, 2018a; Stringer, 2018)	(Pangbourne et al., 2020; Polydoropoulou et al., 2020; Smith, Sochor, & Karlsson, 2018a; Stringer, 2018; Vitkauskaite & Vaiciukynaite, 2020; Zhao et al., 2020)

(continued on next page)

Table 4 (*continued*)

Dimension	BMC's factor	BMC's building block	Strands of MaaS literature	
			MaaS scenarios	Development factors
Platform functionalities	App, website, social media	Channels	(Enoch, 2018; Enoch et al., 2020; Vaddadi et al., 2020)	(Corazza & Carassiti, 2021; Kamargianni et al., 2016; Pangbourne et al., 2020; Polydoropoulou et al., 2020; Stringer, 2018; Vitkauskaite & Vaiciukynaite, 2020; Wong et al., 2020; Zhao et al., 2020)
	Seamless, integrated, multimodal travel experience	Value Propositions	(Enoch, 2018; Enoch et al., 2020; Smith, Sochor, & Karlsson, 2018a; Vaddadi et al., 2020)	(Corazza & Carassiti, 2021; Kamargianni et al., 2016; Mulley, 2017; Pangbourne et al., 2020; Polydoropoulou et al., 2020; Smith, Sochor, & Karlsson, 2018a; Stringer, 2018; Tinnilä, 2016; Vitkauskaite & Vaiciukynaite, 2020; Wong et al., 2020; Zhao et al., 2020)
	Travel planning, booking, ticketing and payment	Value Propositions	(Enoch, 2018; Enoch et al., 2020; Smith, Sochor, & Karlsson, 2018a; Vaddadi et al., 2020)	(Corazza & Carassiti, 2021; Kamargianni et al., 2016; Polydoropoulou et al., 2020; Smith, Sochor, & Karlsson, 2018a; Stringer, 2018; Tinnilä, 2016; Vitkauskaite & Vaiciukynaite, 2020; Wong et al., 2020; Zhao et al., 2020)
	One-stop-shop for travel services	Value Propositions	(Vaddadi et al., 2020)	(Corazza & Carassiti, 2021; Kamargianni et al., 2016; Stringer, 2018; Wong et al., 2020)
	Service personalisation	Value Propositions	(Enoch, 2018; Enoch et al., 2020)	(Corazza & Carassiti, 2021; Kamargianni et al., 2016; Pangbourne et al., 2020; Polydoropoulou et al., 2020; Vitkauskaite & Vaiciukynaite, 2020; Wong et al., 2020; Zhao et al., 2020)
	Data-driven insights	Value Propositions	(Enoch, 2018; Enoch et al., 2020)	(Kamargianni et al., 2016; Mulley, 2017; Pangbourne et al., 2020)
	Social benefits	Value Propositions	(Enoch, 2018; Enoch et al., 2020; Smith, Sochor, & Karlsson, 2018a)	(Enoch, 2018; Mulley, 2017; Pangbourne et al., 2020; Polydoropoulou et al., 2020; Smith, Sochor, & Karlsson, 2018a; Tinnilä, 2016; Wong et al., 2020; Zhao et al., 2020)
	Customer support	Key Activities		(Polydoropoulou et al., 2020; Vitkauskaite & Vaiciukynaite, 2020)
	Third-party retailers	Channels		(Polydoropoulou et al., 2020; Vitkauskaite & Vaiciukynaite, 2020)
Public governance	Public subsidies	Revenue Streams	(Enoch, 2018; Enoch et al., 2020; Smith, Sochor, & Karlsson, 2018a; Vaddadi et al., 2020)	(Corazza & Carassiti, 2021; Pangbourne et al., 2020; Polydoropoulou et al., 2020; Smith, Sochor, & Karlsson, 2018a; Tinnilä, 2016; Wong et al., 2020)
	Investment and operational cost subsidy	Cost Structure	(Enoch, 2018; Enoch et al., 2020)	(Polydoropoulou et al., 2020; Smith, Sochor, & Karlsson, 2018a; Stringer, 2018; Tinnilä, 2016; Wong et al., 2020)
Incentives for MaaS providers	Commission on ticket selling	Commission on ticket selling		(Polydoropoulou et al., 2020; Smith, Sochor, & Karlsson, 2018a)
	Revenue packages	Revenue Streams	(Enoch, 2018)	(Corazza & Carassiti, 2021; Pangbourne et al., 2020; Polydoropoulou et al., 2020; Stringer, 2018; Tinnilä, 2016; Vitkauskaite & Vaiciukynaite, 2020; Wong et al., 2020)
	Data reselling	Revenue Streams		(Corazza & Carassiti, 2021; Polydoropoulou et al., 2020)
Incentives for users	Loyalty programs	Customer Relationships		(Corazza & Carassiti, 2021; Polydoropoulou et al., 2020; Vitkauskaite & Vaiciukynaite, 2020)
	Discounts	Customer Relationships	(Enoch, 2018)	(Corazza & Carassiti, 2021; Kamargianni et al., 2016; Pangbourne et al., 2020; Polydoropoulou et al., 2020; Stringer, 2018; Vitkauskaite & Vaiciukynaite, 2020)
Cyber security	Data security and privacy-related cost	Cost Structure	(Enoch, 2018)	(Corazza & Carassiti, 2021; Pangbourne et al., 2018)

Privacy and security, not in depth

References

Adjust. (2024). Wunder Mobility. https://www.wundermobility.com/marketplace/adjust (accessed March 8, 2024).

Ahmed, M., & Pathan, A. S. K. (2020). False data injection attack (FDIA): An overview and new metrics for fair evaluation of its countermeasure. *Complex Adaptive Systems Modeling, 8*, 1–14. https://doi.org/10.1186/s40294-020-00070-w

Alonso-González, M. J., Hoogendoorn-Lanser, S., van Oort, N., Cats, O., & Hoogendoorn, S. (2020). Drivers and barriers in adopting mobility as a service (MaaS) – A latent class cluster analysis of attitudes. *Transportation Research Part A Policy and Practice, 132*, 378–401. https://doi.org/10.1016/j.tra.2019.11.022

Alyavina, E., Nikitas, A., & Njoya, E. T. (2022). Mobility as a service (MaaS): A thematic map of challenges and opportunities. *Research in Transportation Business and Management, 43*, Article 100783. https://doi.org/10.1016/j.rtbm.2022.100783

Amblard, F., & Quattrociocchi, W. (2018). Simulating social complexity: social networks and spatial distribution. In B. Edmonds, & R. Meyer (Eds.), *Simulating Complex* (second, pp. 763–800).

Angela Sasse, M., & Rashid, A. (2019). *Human factors knowledge area*.

Aromataris, E., Fernandez, R., Godfrey, C. M., Holly, C., Khalil, H., & Tungpunkom, P. (2015). Summarizing systematic reviews: Methodological development, conduct and reporting of an umbrella review approach. *International Journal of Evidence-Based Healthcare, 13*, 132–140. https://doi.org/10.1097/XEB.0000000000000055

Bale, C. S. E., Varga, L., & Foxon, T. J. (2015). Energy and complexity: New ways forward. *Applied Energy, 138*, 150–159. https://doi.org/10.1016/j.apenergy.2014.10.057

Bizgan, L., Hollings, P., & Reynolds, M. (2020). *Mobility as a service (MaaS) acceptability research - a report by IpsosMORI for the Department for Transport*.

Buckley, R. P., Arner, D. W., Zetzsche, D. A., & Selga, E. (2019). The dark side of digital financial transformation: The new risks of FinTech and the rise of TechRisk. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3478640

Burnap, P. (2019). *Risk Management & Governance Knowledge Area Issue*.

Bushell, J., Merkert, R., & Beck, M. J. (2022). Consumer preferences for operator collaboration in intra- and intercity transport ecosystems: Institutionalising platforms to facilitate MaaS 2.0. *Transportation Research Part A Policy and Practice, 160*, 160–178. https://doi.org/10.1016/j.tra.2022.04.013

Butler, L., Yigitcanlar, T., & Paz, A. (2021). Barriers and risks of mobility-as-a-service (MaaS) adoption in cities: A systematic review of the literature. *Cities, 109*, Article 103036. https://doi.org/10.1016/j.cities.2020.103036

Caballini, C., Olivari, E., Gasparini, C., & Dalla, C. B. (2023). The spread of MaaS initiatives in Europe: The leading role of public governance emerging from an Italian regional application. *Sustain, 15*, 13413. https://doi.org/10.3390/su151813413

Cardenas, A., & Cruz, S. (2019). *Cyber-physical systems security knowledge area*. Cyber Secur Body Knowl.

Cisterna, C., Giorgione, G., & Viti, F. (2021). Explorative analysis of potential MaaS customers: An agent-based scenario. In *, 184. Procedia Comput. Sci* (pp. 629–634). Elsevier. https://doi.org/10.1016/j.procs.2021.03.078.

Cisterna, C., Bigi, F., Tinessa, F., & Viti, F. (2022). Analysis of MaaS membership attributes: An agent-based approach. In *, 62. Transp. Res. Procedia* (pp. 483–490). Elsevier B.V. https://doi.org/10.1016/j.trpro.2022.02.060.

Corazza, M. V., & Carassiti, G. (2021). Investigating maturity requirements to operate mobility as a service: The Rome case. *Sustain, 13*, 8367. https://doi.org/10.3390/su13158367

Cottrill, C. D. (2020). MaaS surveillance: Privacy considerations in mobility as a service. *Transportation Research Part A Policy and Practice, 131*, 50–57. https://doi.org/10.1016/j.tra.2019.09.026

Coventry, L., Briggs, P., Blythe, J., & Tran, M. (2014). *Using behavioural insights to improve the public ' s use of cyber security best practices improve the public ' s use of cyber*.

Department for Transport. (2023). *Future of Transport: supporting rural transport innovation*.

Department of Transport. (2020). *Future of Transport Regulatory Review - Summary of Responses*.
Docherty, I. (2000). Rail transport policy-making in UK passenger Transport authority areas. *Journal of Transport Geography, 8*, 157–170. https://doi.org/10.1016/S0966-6923(00)00008-9
Duan, S. X., Tay, R., Molla, A., & Deng, H. (2022). Predicting mobility as a service (MaaS) use for different trip categories: An artificial neural network analysis. *Transportation Research Part A Policy and Practice, 166*, 135–149. https://doi.org/10.1016/j.tra.2022.10.014
Dulskaia, I., & Bellini, F. (2023). New Business Models and Partnerships for Sustainable Mobility and Transport Sector. In *, 319*. *Smart Innov. Syst. Technol* (pp. 279–302). Singapore: Springer. https://doi.org/10.1007/978-981-19-6962-1_15.
Enoch, M. (2018). *Mobility as a service (MaaS) in the UK: Change and its implications*.
Enoch, M., & Potter, S. (2023). MaaS (mobility as a service) market futures explored. *Transport Policy, 134*, 31–40. https://doi.org/10.1016/j.tranpol.2023.02.007
Enoch, M., Cross, R., Potter, N., Davidson, C., Taylor, S., Brown, R., et al. (2020). Future local passenger transport system scenarios and implications for policy and practice. *Transport Policy, 90*, 52–67. https://doi.org/10.1016/j.tranpol.2020.02.009
European Commission. (2024). Digital Scoreboard - Data & Indicators. https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/key-indicators/charts (accessed October 20, 2022).
Farmer, J. D., & Foley, D. (2009). The economy needs agent-based modelling. *Nature, 460*, 685–686. https://doi.org/10.1038/460685a
Flowbird - Urban intelligence. https://www.flowbird.group/, (2024) (accessed March 8, 2024).
Gkemou, M. (2018). MyCorridor Use Cases, Deliverable 1.1 MyCorridor (Mobility as a Service in a multimodal European cross-border Corridor) project (G.A.: 723384). http://mycorridor.eu/.
Greenhalgh, T., & Peacock, R. (2005). Effectiveness and efficiency of search methods in systematic reviews of complex evidence: Audit of primary sources. *British Medical Journal, 331*, 1064–1065. https://doi.org/10.1136/bmj.38636.593461.68
Habibzadeh, H., Nussbaum, B. H., Anjomshoa, F., Kantarci, B., & Soyata, T. (2019). A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. *Sustainable Cities and Society, 50*, Article 101660. https://doi.org/10.1016/j.scs.2019.101660
Hensher, D. A. (2017). Future bus transport contracts under a mobility as a service (MaaS) regime in the digital age: Are they likely to change? *Transportation Research Part A Policy and Practice, 98*, 86–96. https://doi.org/10.1016/j.tra.2017.02.006
Ho, C. Q. (2022). Can MaaS change users' travel behaviour to deliver commercial and societal outcomes? *Transportation Research Part A: Policy and Practice, 165*, 76–97. https://doi.org/10.1016/j.tra.2022.09.004
Hodson, M., Lockhart, A., & McMeekin, A. (2023). How have digital mobility platforms responded to COVID-19 and why does this matter for 'the urban'? *Urban Studies*. https://doi.org/10.1177/00420980231194891
Jittrapirom, P., Caiati, V., Feneri, A. M., Ebrahimigharehbaghi, S., Alonso-González, M. J., & Narayan, J. (2017). Mobility as a service: A critical review of definitions, assessments of schemes, and key challenges. *Urban Planning, 2*, 13–25. https://doi.org/10.17645/up.v2i2.931
Jittrapirom, P., Marchau, V., van der Heijden, R., & Meurs, H. (2020). Future implementation of mobility as a service (MaaS): Results of an international Delphi study. *Travel Behaviour and Society, 21*, 281–294. https://doi.org/10.1016/j.tbs.2018.12.004
Kamargianni, M., Li, W., Matyas, M., & Schäfer, A. (2016). *A Critical Review of New Mobility Services for Urban Transport. Transp. Res. Procedia. 14* pp. 3294–3303). Elsevier. https://doi.org/10.1016/j.trpro.2016.05.277
Köhler, J., Turnheim, B., & Hodson, M. (2020). Low carbon transitions pathways in mobility: Applying the MLP in a combined case study and simulation bridging analysis of passenger transport in the Netherlands. *Technological Forecasting and Social Change, 151*, Article 119314. https://doi.org/10.1016/j.techfore.2018.06.003
Kurmanova, L., Nurdavliatova, E., Kurmanova, D., Galimova, G., & Khabibullin, R. (2021). Development of digital services and information security of banks. In *ACM Int. Conf. Proceeding Ser., Association for Computing Machinery*. https://doi.org/10.1145/3487757.3490911
Leicester City Council. https://skedgo.com/case-studies/leicester/, (2024) (accessed March 8, 2024).
Liimatainen, H., & Mladenović, M. N. (2018). Understanding the complexity of mobility as a service. *Research in Transportation Business and Management, 27*, 1–2. https://doi.org/10.1016/j.rtbm.2018.12.004
Llp, O. C. (2024). *Mobility as a Service in a multimodal European cross-border Corridor (MyCorridor) Deliverable 7.4 Analysis of legal and regulatory barriers in MaaS*.
Local Government Association. (2021). *The future of public transport and the role of Local Government*.
MaaS. (2021). MaaS-Alliance The Mobility as a Service Alliance. https://maas-alliance.eu/ (accessed July 1, 2022).
Mahood, Q., Van Eerd, D., & Irvin, E. (2014). Searching for grey literature for systematic reviews: Challenges and benefits. *Research Synthesis Methods, 5*, 221–234. https://doi.org/10.1002/JRSM.1106
Matyas, M., & Kamargianni, M. (2019). The potential of mobility as a service bundles as a mobility management tool. *Transportation (Amst), 46*, 1951–1968. https://doi.org/10.1007/s11116-018-9913-4
McTigue, C., Monios, J., & Rye, T. (2018). Identifying barriers to implementation of local transport policy: An analysis of bus policy in Great Britain. *Utilities Policy, 50*, 133–143. https://doi.org/10.1016/j.jup.2017.12.002
Mering, M. (2018). Defining and understanding Grey literature. *Serials Review, 44*, 238–240. https://doi.org/10.1080/00987913.2018.1525239
Mitropoulos, L., Kortsari, A., Mizaras, V., & Ayfantopoulou, G. (2023). Mobility as a service (MaaS) planning and implementation: Challenges and lessons learned. *Future Transportation, 3*, 498–518. https://doi.org/10.3390/futuretransp3020029
Mulley, C. (2017). Mobility as a services (MaaS)–does it have critical mass? *Transport Reviews, 37*, 247–251. https://doi.org/10.1080/01441647.2017.1280932
Office for National Statistics O. (2012). *Eurostat - An overview of the 3 NUTS and 2 LAU layers in the UK. Off Natl Stat - Methodol* (pp. 2011–2014). https://www.ons.gov.uk/methodology/geography/ukgeographies/eurostat (accessed June 22, 2022).
Pangbourne, K., Stead, D., Mladenović, M., & Milakis, D. (2018). The case of mobility as a service: A critical reflection on challenges for urban Transport and mobility governance. In *Gov. Smart Mobil. Transit* (pp. 33–48). Emerald Publishing Limited. https://doi.org/10.1108/978-1-78754-317-120181003.
Pangbourne, K., Mladenović, M. N., Stead, D., & Milakis, D. (2020). Questioning mobility as a service: Unanticipated implications for society and governance. *Transportation Research Part A Policy and Practice, 131*, 35–49. https://doi.org/10.1016/j.tra.2019.09.033
Paré, G., Trudel, M. C., Jaana, M., & Kitsiou, S. (2015). Synthesizing information systems knowledge: A typology of literature reviews. *Information Management, 52*, 183–199. https://doi.org/10.1016/j.im.2014.08.008
Polydoropoulou, A., Pagoni, I., Tsirimpa, A., Roumboutsos, A., Kamargianni, M., & Tsouros, I. (2020). Prototype business models for mobility-as-a-service. *Transportation Research Part A Policy and Practice, 131*, 149–162. https://doi.org/10.1016/j.tra.2019.09.035
Pundir, A., Singh, S., Kumar, M., Bafila, A., & Saxena, G. J. (2022). Cyber-physical systems enabled Transport networks in smart cities: Challenges and enabling Technologies of the new Mobility era. *IEEE Access, 10*, 16350–16364. https://doi.org/10.1109/ACCESS.2022.3147323
Sakai, K. (2019). MaaS trends and policy-level initiatives in the EU. *IATSS Research, 43*, 207–209. https://doi.org/10.1016/j.iatssr.2019.11.001
Sayers, A. (2008). Tips and tricks in performing a systemic review. *The British Journal of General Practice, 58*, 136. https://doi.org/10.3399/bjgp08X277168
Schikofsky, J., Dannewald, T., & Kowald, M. (2020). Exploring motivational mechanisms behind the intention to adopt mobility as a service (MaaS): Insights from Germany. *Transportation Research Part A Policy and Practice, 131*, 296–312. https://doi.org/10.1016/j.tra.2019.09.022
Schneider, P. R., & Koska, T. (2023). *Mobility data for a just transition : The case for multimodal platforms and data-driven transportation planning. Berlin*.
Seamlessly accessible - MoveYou. https://moveyou.com/, (2024) (accessed March 8, 2024).
Slim, K., & Marquillier, T. (2022). Umbrella reviews: A new tool to synthesize scientific evidence in surgery. *Journal of Visceral Surgery, 159*, 144–149. https://doi.org/10.1016/j.jviscsurg.2021.10.001
Smith, G., & Sørensen, C. H. (2023). Public-private MaaS: Unchallenged assumptions and issues of conflict in Sweden. *Research in Transportation Economics, 99*, Article 101297. https://doi.org/10.1016/j.retrec.2023.101297
Smith, G., Sochor, J., & Karlsson, I. C. M. A. (2018a). Mobility as a service: Development scenarios and implications for public transport. *Research in Transportation Economics, 69*, 592–599. https://doi.org/10.1016/j.retrec.2018.04.001
Smith, G., Sochor, J., & Sarasini, S. (2018b). Mobility as a service: Comparing developments in Sweden and Finland. *Research in Transportation Business and Management, 27*, 36–45. https://doi.org/10.1016/j.rtbm.2018.09.004
Sochor, J., Strömberg, H., & Karlsson, I. C. M. (2015). Implementing mobility as a service: Challenges in integrating user, commercial, and societal perspectives. *Transportation Research Record, 2536*, 1–9. https://doi.org/10.3141/2536-01
Solent Future Transport Zone. (2024). *Engineering*. University of Southampton. https://www.southampton.ac.uk/engineering/research/projects/solent-future-transport-zone-theme-1.page (accessed March 22, 2024).
Solent Transport. (2024). Solent Transport. https://solent-transport.com/ (accessed March 22, 2024).
Stringer, G. (2018). *Mobility as a service eighth report of session 2017–19 report, together with formal minutes relating to the report*.
Struben, J., & Sterman, J. D. (2008). Transition challenges for alternative fuel vehicle and transportation systems. *Environment and Planning. B, Planning & Design, 35*, 1070–1097. https://doi.org/10.1068/b33022t
The European Parliament and the Council of the European. (2010). *Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport*.
Tinnilä, M. T. (2016). Towards servitization of mobility –mobility as a service. *International Journal of Business and Technology, 8*, 958–963. https://doi.org/10.17722/ijrbt.v8i2.444
Trafi: Vilnius app. https://www.trafi.com/vilnius-app, (2024) (accessed March 21, 2024).
Trowbridge, A., Sharevski, F., & Westbrook, J. (2018). Malicious user experience design research for cybersecurity. In *ACM Int. Conf. Proceeding Ser.* New York, New York, USA: ACM Press. https://doi.org/10.1145/3285002.3285010.
United Nations. (2017). *Sustainable transport: Sustainable development knowledge platform*. Sustain Dev Knowl Platf.
University of Southampton. (2024). *Solent Future Transport Zone | Engineering*. University of Southampton. https://www.southampton.ac.uk/engineering/research/projects/solent-future-transport-zone-theme-1.page (accessed March 22, 2024).
Urciuoli, L., Männistö, T., Hintsa, J., & Khan, T. (2013). Supply chain cyber security – Potential threats. *International Journal of Information Security, 29*, 51–68. https://doi.org/10.11610/isij.2904

Utriainen, R., & Pöllänen, M. (2018). Review on mobility as a service in scientific publications. *Research in Transportation Business and Management, 27*, 15–23. https://doi.org/10.1016/j.rtbm.2018.10.005

Vaddadi, B., Zhao, X., & Andruetto, C. (2020). *Values of MaaS potential impacts based on representative scenarios*.

van Duinen, R., Filatova, T., Jager, W., & van der Veen, A. (2016). Going beyond perfect rationality: Drought risk, economic choices and the influence of social networks. *The Annals of Regional Science, 57*, 335–369. https://doi.org/10.1007/s00168-015-0699-4

van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior, 75*, 547–559. https://doi.org/10.1016/j.chb.2017.05.038

Vitkauskaite, E., & Vaiciukynaite, E. (2020). Comparative study of business models of European micro-mobility online services. In *, 2020- Decem. Proc. Int. Conf. Electron. Bus* (pp. 55–62).

Wong, Y. Z., Hensher, D. A., & Mulley, C. (2020). Mobility as a service (MaaS): Charting a future context. *Transportation Research Part A Policy and Practice, 131*, 5–19. https://doi.org/10.1016/j.tra.2019.09.030

Wunder Mobility: market-leading software provider for shared mobility operators. https://www.wundermobility.com/, (2024) (accessed March 8, 2024).

Yin, X., Zhu, Y., & Hu, J. (2021). A comprehensive survey of privacy-preserving federated learning: A taxonomy, review, and future directions. *ACM Computing Surveys*, 54. https://doi.org/10.1145/3460427

Zhao, X., Vaddadi, B., Sjöman, M., Hesselgren, M., & Pernestål, A. (2020). Key barriers in MaaS development and implementation: Lessons learned from testing corporate MaaS (CMaaS). *Transportation Research Interdisciplinary Perspectives, 8*, Article 100227. https://doi.org/10.1016/j.trip.2020.100227

Zöschinger, J. (2019). *Design of a sustainability-oriented mobility-as-a-service framework for the City of Munich*. Technische Universität München.