POLYPUBLIE

A systematic review of data privacy in mobility as a service (MaaS)

Zineb Garroussi, Antoine Legrain, Sébastien Gambs, Vincent Gautrais, Brunilde Sanso

Document en libre accès dans PolyPublie
Open Access document in PolyPublie

Date	2025
Type	Article de revue / Article
Version	Version officielle de l'éditeur / Published version
URL de PolyPublie **PolyPublie URL**	https://publications.polymtl.ca/63349/
Évaluation par les pairs **Peer reviewed**	Révisé par les pairs / Refereed
Conditions d'utilisation **Terms of use**	Creative Commons Attribution-Utilisation non commerciale-Pas d'oeuvre dérivée 4.0 International / Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND)
Référence **Citation**	Garroussi, Z., Legrain, A., Gambs, S., Gautrais, V., & Sanso, B. (2025). A systematic review of data privacy in mobility as a service (MaaS). Transportation Research Interdisciplinary Perspectives, 31, 101254 (12 pages). https://doi.org/10.1016/j.trip.2024.101254

Publication officielle
Official publication

Titre de la revue **Journal title**	Transportation Research Interdisciplinary Perspectives (vol. 31)
Maison d'édition **Publisher**	Elsevier
URL officielle **Official URL**	https://doi.org/10.1016/j.trip.2024.101254
Mention légale **Legal notice**	© 2024 Published by Elsevier Ltd. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

Ce fichier a été téléchargé à partir de PolyPublie, le dépôt institutionnel de Polytechnique Montréal
This file has been downloaded from PolyPublie, the institutional repository of Polytechnique Montréal
https://publications.polymtl.ca

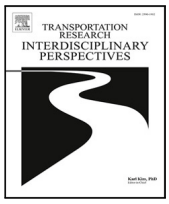
Transportation Research Interdisciplinary Perspectives 31 (2025) 101254



Contents lists available at ScienceDirect

Transportation Research Interdisciplinary Perspectives

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





A systematic review of data privacy in Mobility as a Service (MaaS)

Zineb Garroussi [a,d,*], Antoine Legrain [a,b,d], Sébastien Gambs [c], Vincent Gautrais [e], Brunilde Sansò [a,d]

[a] Polytechnique Montréal, 2900 Edouard-Montpetit Blvd, Université de Montréal Campus, 2500 Polytechnique Road, H3T 1J4, Montréal, Canada
[b] Interuniversity Research Center on Enterprise Networks, Logistics and Transportation (CIRRELT), Andre-Aisenstadt Building, Université de Montréal, P.O. Box 6128, H3C 3J7, Montréal, Canada
[c] Université du Québec à Montréal, Computer science department, 2098 Rue Kimberley, H3C 3P8, Montréal, Canada
[d] Group for Research in Decision Analysis (GERAD), HEC Montréal, 3000, Cote-Sainte-Catherine Road, H3T 2A7, Montréal, Canada
[e] CRDP - Faculty of Law - Université de Montréal, 3101 Ch de la Tour, H3T 1J7, Montréal, Canada

ARTICLE INFO

Keywords:
Mobility as a Service (MaaS)
Privacy
Federated learning
Blockchain
Anonymization
Privacy legislation

ABSTRACT

Mobility as a Service (MaaS) integrates various transportation modes to offer seamless urban mobility solutions. However, the extensive collection and sharing of user data on MaaS platforms pose significant privacy challenges. This systematic review identifies key data privacy concerns, evaluates current privacy-preserving technologies, and explores the role of regulatory frameworks in ensuring user privacy in MaaS systems. Using the PRISMA framework, a comprehensive literature search across Web of Science, Elsevier, and IEEE Xplore databases resulted in the selection of 32 studies for detailed analysis.

The review is structured around three main themes: (1) Privacy-Preserving Techniques, including anonymization strategies (k-anonymity, differential privacy, obfuscation), encryption methods (blockchain, cryptographic protocols), federated learning for decentralized data processing, and advanced algorithms for optimizing privacy budgets and balancing utility-privacy trade-offs; (2) User Trust and Privacy Perceptions, highlighting that trust in service providers is essential for MaaS adoption, privacy concerns may impact adoption but do not necessarily prevent it (the "privacy paradox"), and awareness of data misuse affects user trust and willingness to adopt MaaS; and (3) Regulatory Frameworks, focusing on the importance of GDPR compliance to ensure strict data protection through consent and transparency, and embedding privacy-by-design principles within MaaS architectures to safeguard user data from the outset.

This review emphasizes the need for a holistic approach, integrating technological innovation, user-centered design, and strong regulatory oversight to effectively address privacy challenges in MaaS. Future research should focus on developing scalable privacy frameworks that protect user data without compromising operational efficiency.

1. Introduction

Mobility as a Service (MaaS) has emerged as a modern solution to the growing transportation needs in rapidly urbanizing cities. It integrates multiple transportation modes – such as public transit, ride-sharing, bike-sharing and car rentals – into a unified digital platform, enhancing flexibility and efficiency in urban travel. The MaaS market is expanding rapidly, with projections estimating its value will reach $300 billion by 2030 (Asensio et al., 2022). MaaS has the potential to reduce the dependence to private car, ease traffic congestion and promote sustainable urban mobility, making it a key focus for transportation engineers and planners seeking to create efficient and integrated urban systems (Utriainen and Pöllänen, 2018). Despite its benefits, MaaS presents significant data privacy challenges. In particular, MaaS platforms collect and process large amounts of personal data, including real-time location information, travel patterns and user preferences. This data is crucial for optimizing routes, managing traffic flow and improving service delivery—core objectives in transportation engineering, which strives to enhance mobility, accessibility, safety and sustainability. The principles of efficiency and user-centric design are central to MaaS, as data allows for personalized services and optimized transit operations.

* Corresponding author at: Polytechnique Montréal, 2900 Edouard-Montpetit Blvd, Université de Montréal Campus, 2500 Polytechnique Road, H3T 1J4, Montréal, Canada.
E-mail addresses: zineb.garroussi@polymtl.ca (Z. Garroussi), antoine.legrain@polymtl.ca (A. Legrain), gambs.sebastien@uqam.ca (S. Gambs), vincent.gautrais@umontreal.ca (V. Gautrais), brunilde.sanso@polymtl.ca (B. Sansò).

https://doi.org/10.1016/j.trip.2024.101254
Received 6 March 2024; Received in revised form 13 October 2024; Accepted 20 October 2024
Available online 11 March 2025
2590-1982/© 2025 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/).

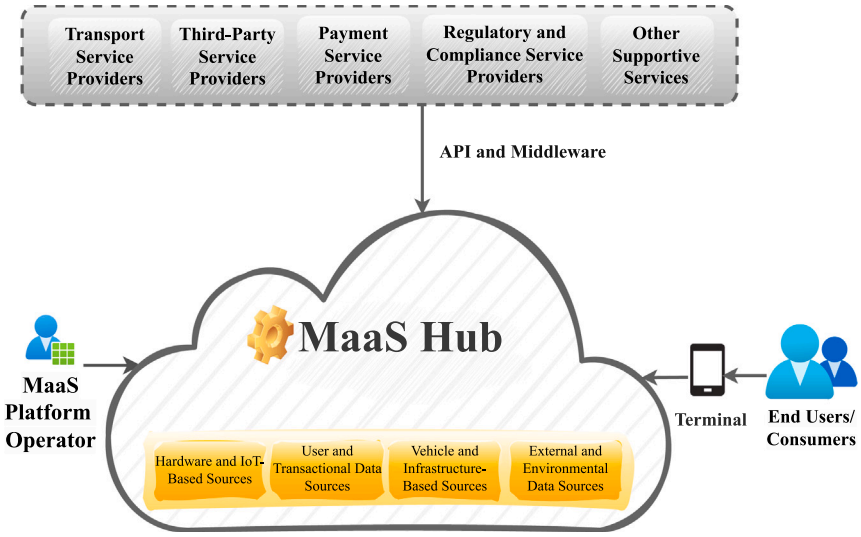


Fig. 1. MaaS Hub.

However, the usage of sensitive information also raises privacy concerns. For instance, if it is not correctly manage it could result in unauthorized access, data breaches and misuse, undermining the principles of safety and equity in transportation systems. Furthermore, the methods used in transportation planning, such as traffic flow analysis and geospatial analysis, depend heavily on the accurate collection of such data. Without proper privacy safeguards, the potential misuse of this information can erode public trust. Therefore, privacy protection has become a top priority for all involved – users, transportation authorities and other stakeholders in urban mobility – to ensure the continued success and sustainability of MaaS platforms (Lund et al., 2017).

These concerns are further complicated by the interconnected nature of MaaS systems in which a vulnerability in one service can affect the entire transportation network, leading to operational disruptions and long-term planning inefficiencies. Thus, integrating multiple transportation services across a single platform creates complex data-sharing environments, increasing the risk of privacy breaches. For transportation engineers, ensuring the protection of user privacy is as critical as optimizing traffic flow and designing efficient infrastructure (Becker et al., 2020; Enoch and Potter, 2023).

Given the limitations in the current MaaS literature, this systematic review aims to address the following key research question: "*What technologies are used to protect data privacy in the MaaS ecosystem, and what are the implications of regulatory frameworks on these practices?*"

The outline of the paper is as follows. First in Section 2, we provide an overview of the background and key components of the MaaS ecosystem, highlighting core elements and data privacy challenges. In Section 3, we review the methodology used in conducting this systematic review, detailing the literature search, inclusion/exclusion criteria and analysis process. Afterwards in Section 4, we present the key results of the review, including main findings related to privacy-preserving technologies, regulatory frameworks and user trust in MaaS before discussing in Section 5 the implications of the findings, identifying research gaps and suggesting future research directions. Finally in Section 6, we concludes by summarizing the key contributions of this systematic review and outlining the practical applications of the findings.

2. Background

The MaaS ecosystem is a complex network that integrates various stakeholders, services and technologies to deliver user-centric transportation solutions. This section provides an overview of the MaaS ecosystem, focusing on its core components and the flow of interactions within the system. It also addresses the key challenges related to data privacy, emphasizing how privacy concerns intersect with engineering practices to promote sustainable and efficient urban mobility.

2.1. Core components and data flow in MaaS

MaaS ecosystem comprises several key components that interact to provide a unified mobility service to users:

- The **MaaS Platform Operator** is the central entity responsible for orchestrating services, integrating data sources and coordinating stakeholders. The operator ensures the seamless operation of the ecosystem, providing a cohesive experience for users.
- The **Transport Service Providers**, including public transportation authorities, ride-sharing, ride-hailing companies and micro-mobility services like bike-sharing. They offer diverse mobility options accessible through the MaaS platform.
- The **Third-Party Service Providers** enhance the MaaS ecosystem by offering additional services such as insurance, customer support and data analytics, which add value to the overall user experience.
- The **Payment Service Providers**, including financial institutions and payment gateways, facilitate transactions within the MaaS ecosystem, ensuring smooth and secure payment processes for users.
- The **Regulatory and Compliance Bodies** establish and enforce data privacy regulations, safety standards and other legal requirements, ensuring that the MaaS ecosystem operates within the bounds of the law (Cottrill, 2020).

Fig. 1 illustrates the flow of interactions within a MaaS ecosystem, in which the MaaS Platform Operator coordinates the integration of services, data sources and stakeholders within the MaaS Hub. When a customer uses a terminal, such as a smartphone, tablet or other device, to book a trip, this request is processed through the MaaS Hub. The MaaS Hub leverages APIs and middleware to communicate with a wide range of services, including transport service providers, third-party service providers, payment service providers, regulatory and compliance service providers as well as other supportive services. The data from these providers – such as hardware and IoT-based sources, user and transactional data, vehicle and infrastructure data, and external environmental data – are integrated and processed within the hub. This integration enables the MaaS Hub to deliver a seamless

and personalized solution to the customer, ensuring that their mobility needs are met efficiently and effectively. The entire system is designed to provide users with a streamlined experience, connecting them to all transport options through a single platform (Cottrill, 2020).

2.2. Data privacy and engineering in urban mobility

Data privacy is a critical consideration in transportation operations and planning. In particular, services such as ride-hailing and public transit coordination rely on the use of sensitive user data to optimize routes and schedules, but the sharing of this data across multiple service providers presents significant privacy risks. Balancing transportation methodologies, such as route optimization, with privacy concerns is essential for improving traffic management without compromising user data security (Belletti and Bayen, 2017).

The integration of these various components into the MaaS ecosystem introduces specific privacy challenges (Casquero et al., 2022). Indeed, as data from different sources – such as user transactions, vehicle sensors and external environmental inputs – flows through the MaaS Hub, ensuring both the privacy and security of this information becomes increasingly complex. Protecting sensitive user information while facilitating data sharing among service providers demands robust privacy frameworks and strict adherence to data protection regulations. The governance of these complex data flows, particularly with the involvement of AI-driven processes, requires a hybrid approach, combining human oversight with algorithmic decision-making to ensure compliance with privacy standards (Servou et al., 2023). Additionally, the use of APIs and middleware, critical for enabling interoperability, introduces risks of data breaches and unauthorized access. Addressing these challenges is vital to maintaining user trust and ensuring the long-term viability of MaaS ecosystems.

Public transit coordination within MaaS platforms similarly depends on the exchange of data between transit agencies and other service providers. Indeed, sharing data on passenger demand, vehicle availability and route predictions is essential for optimizing transit schedules. Privacy-enhancing technologies such as obfuscation and differential privacy play a crucial role in ensuring that real-time tracking and predictions comply with regulations without compromising operational efficiency. MaaS also supports broader urban mobility goals, such as reducing private car ownership, promoting multimodal travel and improving access to public transit (Chen et al., 2023).

Furthermore, transportation-specific methodologies, such as urban congestion management, intersect also with data privacy challenges. Effective congestion management requires the collection and analysis of vehicle and commuter data, thus incorporating privacy-preserving strategies into these frameworks is necessary to protect user data while supporting efficient urban mobility (Athanasopoulou et al., 2022).

3. Methodology

Systematic reviews have become an essential methodology due to their structured and replicable approach (Nasser, 2020).

One key strength of this approach is its ability to minimize bias by adhering to a predefined protocol. In particular, systematic quantitative reviews help to visually map patterns and trends, helping identify knowledge gaps and guiding future research to address key questions. In what follows, we specifically explain the methodology on the application of the PRISMA framework for systematic reviews (Moher et al., 2009).

3.1. PRISMA framework

The Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) is a well-established methodology designed to ensure transparency and rigor in systematic reviews. PRISMA provides a structured approach that guides researchers through each step of the review process, from identification and screening to the inclusion of studies.

For this work, a comprehensive literature search was conducted across three academic databases, namely Web of Science, Elsevier and IEEE Xplore, utilizing the search string (“Mobility as a Service” OR “Mobility-as-a-Service” OR “MaaS” OR “On-Demand Mobility” OR “Shared Mobility” OR “Transportation as a Service” OR “Smart Mobility” OR “Integrated Mobility Services”) AND (“Privacy” OR “Data Privacy”). The search fields were restricted to the title, abstract and keywords, as illustrated in Fig. 2. This process initially yielded a total of 1587 records, which were managed using Zotero, a reference management software. After the removal of 132 duplicate records, the remaining articles were screened based on their titles and abstracts. More precisely, the inclusion and exclusion criteria applied during the screening process are detailed in the next subsection.

3.2. Inclusion and exclusion criteria

This systematic review applied specific inclusion and exclusion criteria to ensure relevance and focus on data privacy within the MaaS ecosystem. Searches were conducted in Web of Science, Elsevier, and IEEE Xplore databases using our predefined keywords, and all retrieved records were downloaded without applying initial filters. After merging the files into a single dataset, 132 duplicate entries were removed. A preliminary screening of titles excluded 506 studies that mentioned keywords but were unrelated to MaaS, such as those focused on passenger safety or general mobility topics. Abstracts and keywords of the remaining articles were then reviewed, leading to the exclusion of 38 additional studies, including those addressing cybersecurity or safety without a clear emphasis on data privacy in MaaS. Following this process, 911 studies were retained, though many addressed peripheral topics rather than core issues of data privacy. The most frequent themes among excluded articles included digital twin technologies, cybersecurity, autonomous vehicles (the majority of exclusions), social impacts of MaaS, and general adoption barriers. Studies focusing on the physical aspects of mobility, such as infrastructure or autonomous vehicles, or on broader topics like cybersecurity or smart mobility without a clear emphasis on data privacy were also excluded. Additionally, studies concentrating on non-MaaS-related transportation modes or those that narrowly focused on specific services within MaaS, such as ride-hailing or bike-sharing, without considering the integrated, multi-modal nature of the MaaS ecosystem, were removed. The final selection focused on studies published between 2015 and 14 August 2024, written in English, available in full-text online, and directly addressing data privacy in MaaS.

4. Results

This section presents the main results of the systematic review, starting with an overview of selected studies, followed by an analysis of key research areas and central themes regarding data privacy in MaaS ecosystems.

4.1. Overview of selected studies

The earliest article retrieved by the databases on data privacy in MaaS was published in 2017, indicating that while the concept of MaaS originated in 2014 (Kayikci and Kabadurmus, 2022), focused research on data privacy within this field did not emerge until three years later. Fig. 3 illustrates the trend of publications from 2017 to 14 August

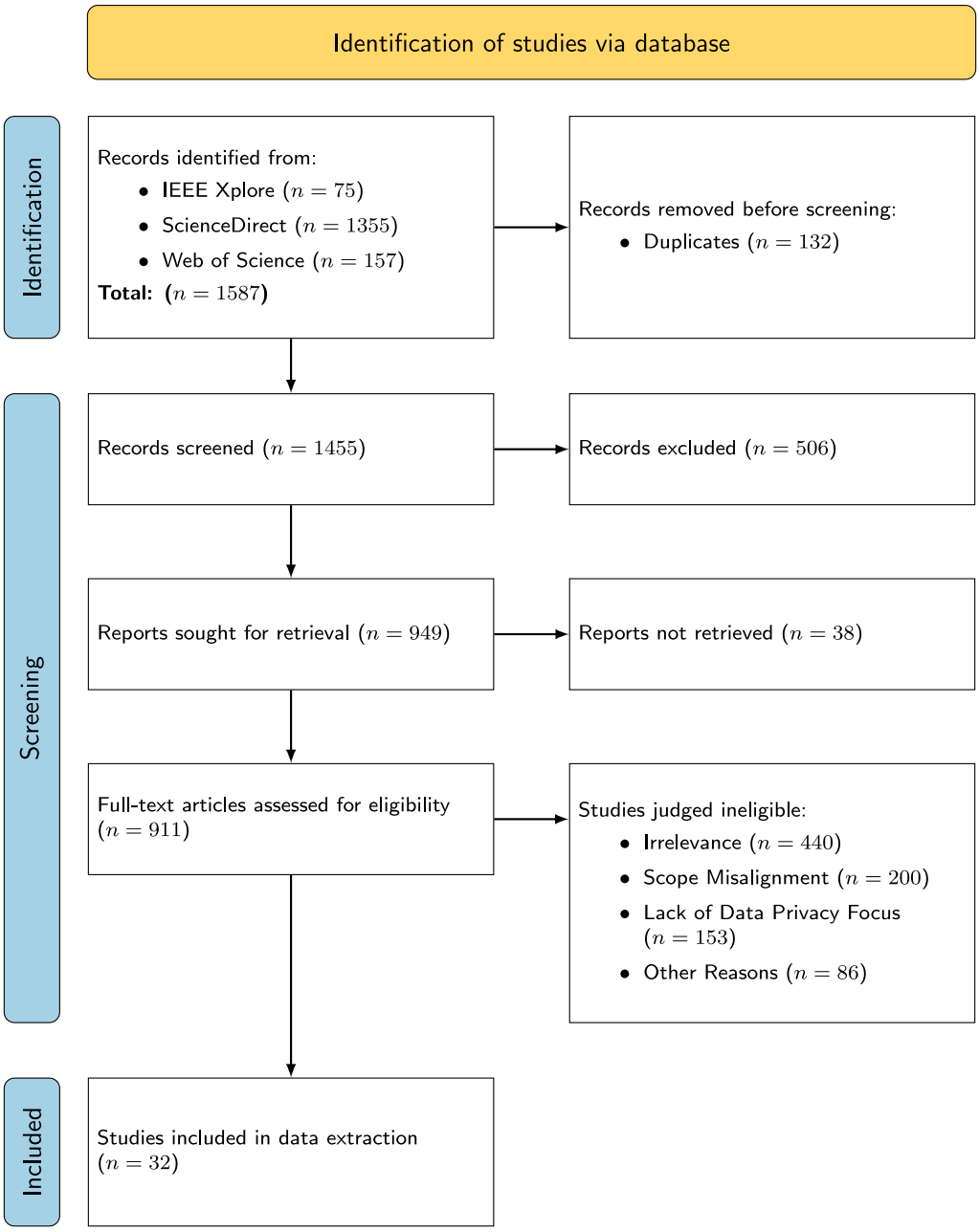


Fig. 2. The PRISMA flowchart. *Source:* Adapted from Moher et al. (2009).

2024, showing a gradual increase in the number of studies. In 2023, relevant publications peaked at 8, reflecting the growing academic and regulatory interest in addressing data privacy concerns as the MaaS ecosystem continued to evolve. This trend aligns with the rising awareness and need for stringent laws and regulations to protect user data in the expanding digital mobility landscape (Cottrill, 2020).

The bar chart shown in Fig. 4 provides a visualization of the distribution of publications on data privacy in MaaS across various research areas. The highest concentration of studies is found in the "Transportation" research area, with around 25 studies, emphasizing the central role of transportation research in the development and analysis of MaaS. "Computer Science" and "Engineering" also feature prominently, each contributing a significant number of studies. In contrast, "Automation & Control Systems" and "Telecommunications" have a moderate presence. Meanwhile, "Business & Economics" and "Operations Research & Management Science", are less represented but their presence highlights the economic implications and operational strategies necessary for effective MaaS deployment. However, some studies could belong to multiple research areas, illustrating the cross-disciplinary nature of research in MaaS and the necessity of integrating knowledge and methodologies from various fields to comprehensively address the multifaceted challenges of data privacy in MaaS ecosystems.

4.2. Main topics

This systematic review identified four main topics critical to understanding data privacy challenges in MaaS: Decision-Making, Law and Policy, Privacy Perception and Technological Tools as shown in Table 1. Decision-Making, representing 21.88% of the studies, focuses

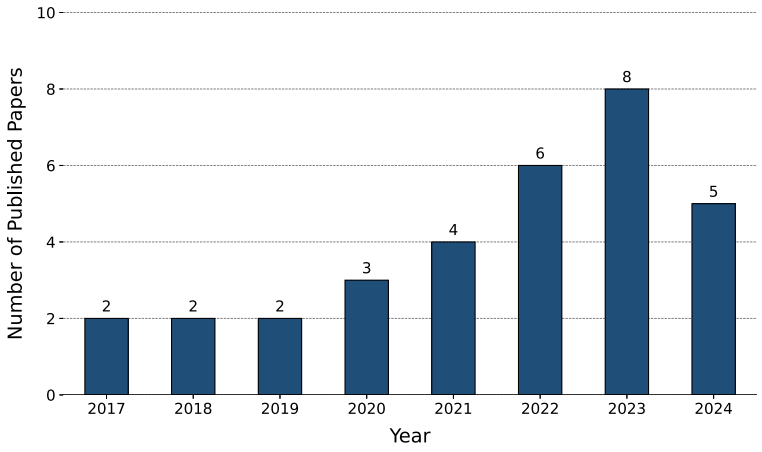


Fig. 3. Number of published papers per year (data collected on 14 August 2024).

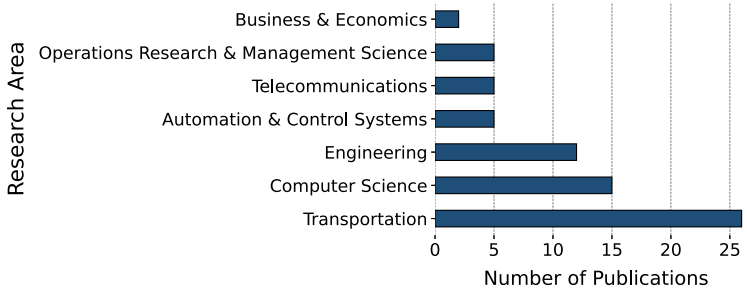


Fig. 4. Number of published papers by Research Area (Data collected on 14 August 2024).

Table 1
Distribution of studies by topic.

Topic	Number of studies	Percentage (%)
Decision-Making	7	21.88%
Law and Policy	3	9.38%
Privacy Perception	6	18.75%
Technological Tools	16	50.00%

on the strategic processes that stakeholders use to balance privacy with operational needs, highlighting the importance of informed choices in managing data privacy risks. Law and Policy, comprising 9.38% of the studies, explores the influence of legal frameworks, such as the GDPR, on the development and implementation of privacy-preserving measures within MaaS systems, underscoring the necessity of robust regulatory support. Privacy Perception, accounting for 18.75% of the studies, examines user attitudes towards data privacy, emphasizing how privacy concerns impact user trust and adoption of MaaS solutions, thus guiding strategies to enhance user confidence in these platforms. Technological Tools, the largest category at 50.00%, delves into the technological innovations, such as federated learning, that are crucial for addressing the complex data privacy issues within MaaS. The distribution of studies across these topics illustrates the need for a multidisciplinary approach that combines strategic decision-making, strong legal frameworks, user trust and cutting-edge technology to effectively manage and protect data privacy in the MaaS ecosystem. In the review, the publications were also categorized by type, with the majority being journal research papers (17 studies), followed by conference research papers (10 studies). Additionally, there were 2 review journal papers, 1 book chapter and 1 systematic literature journal paper.

The rest of this section presents an overview of 32 studies mapped in Fig. 5, whose findings can be divided into three dimensions: Privacy-Preserving Techniques, User Trust and Privacy Perceptions as well as Regulatory Frameworks. Each dimension encapsulates various strategies and approaches, illustrating how data privacy is managed within MaaS systems. In what follows, we group our findings into two dimensions: one concerning Privacy-Preserving Techniques, and the other encompassing both User Trust and Privacy Perception along with Regulatory Frameworks.

4.3. Privacy preserving techniques

4.3.1. Anonymization strategies

Anonymization strategies are crucial to safeguard privacy within the MaaS ecosystem. The MobiDataLab project (Chevallier et al., 2023) highlights the implementation of advanced anonymization techniques, such as k-anonymity (Samarati and Sweeney, 2018) and differential privacy (Dwork and Roth, 2014), to protect personal mobility data while adhering to the FAIR principles (Findable, Accessible, Interoperable and Reusable). k-anonymity aims to prevent re-identification by ensuring that each data record is indistinguishable from at least $k-1$ other records, thereby reducing the risk of linking individual data points back to specific users (Samarati and Sweeney, 2018). Differential privacy, however, has become increasingly significant due to its strong mathematical guarantees. By adding controlled noise to data queries, differential privacy ensures that the inclusion or exclusion of any single individual's data does not significantly affect the results, thus protecting user privacy at the statistical level (Dwork and Roth, 2014). This technique is particularly valuable in the MaaS ecosystem, where it enables the analysis of aggregated mobility data without compromising individual privacy, making it a powerful tool in balancing data utility with privacy concerns. These strategies ensure that data shared among stakeholders is both useful and secure, meeting stringent regulations like the EU's GDPR (Chris Jay Hoofnagle and Borgesius, 2019). The project addresses the challenges posed by the regular nature of mobility data, which is particularly susceptible to re-identification,

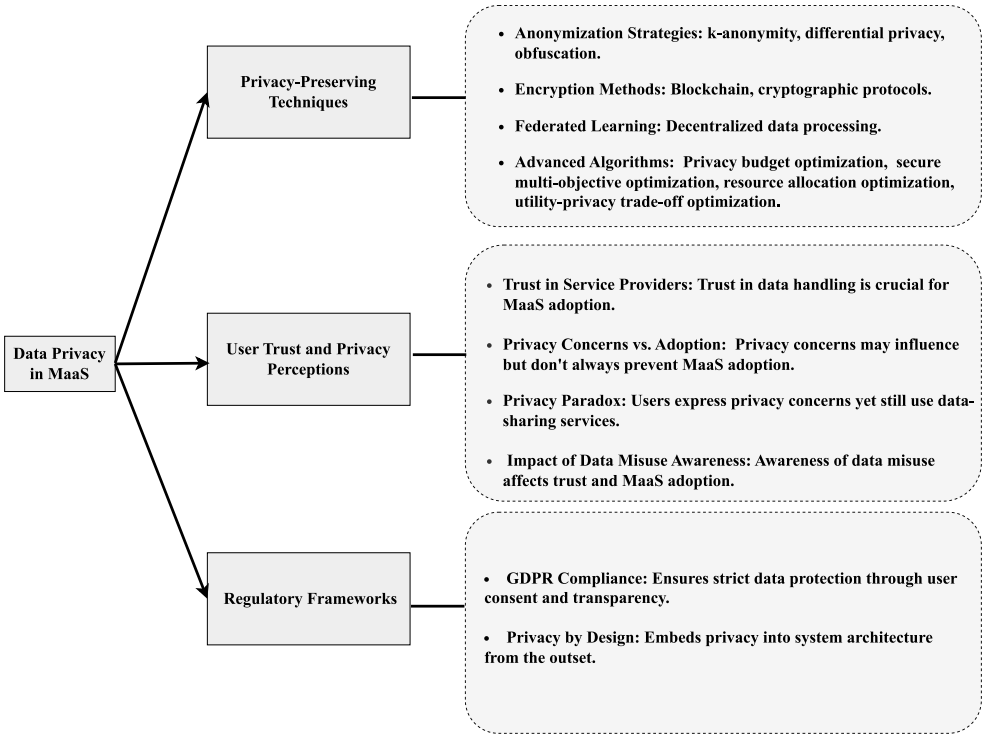


Fig. 5. Summary of studies.

by integrating these anonymization methods within a FAIR-compliant framework.

In another study (Martelli et al., 2021), the impact of privacy-preserving techniques on the performance of mobility-sharing systems is explored, with a focus on location data privacy. The research examines how different anonymization methods, including k-anonymity, obfuscation and cloaking, affect the efficiency of trip-matching algorithms used in ride-sharing applications. While these techniques are essential for safeguarding users' location data, they introduce trade-offs in system performance, such as increased travel distances and longer waiting times. However, the study suggests that these impacts can be mitigated if users accept more flexible travel options.

Building on these anonymization strategies, the privacy-aware zero interaction smart mobility system (Righini et al., 2022) introduces a zero-interaction approach within a privacy-by-design framework. The system, that rely on Bluetooth Low Energy (BLE) technology, avoids the collection of unnecessary personal data. The architecture, based on a microservices design, ensures that personal and session data are stored separately with stringent encryption and anonymization measures. This approach preserves user privacy while maintaining operational efficiency, demonstrating how privacy-preserving techniques can be implemented without compromising the usability of public transport services.

Another approach to anonymization is introduced in a study focused on transport network data sharing (He and Chow, 2019). The research presents a privacy control algorithm based on information-theoretic k-anonymity, designed to generate synthetic data that maximizes anonymity while maintaining high utility. By using tour generation and probability diffusion techniques, the algorithm allows private operators to share valuable data with public agencies without risking reverse engineering of their operational strategies. This approach represents a significant advancement in protecting sensitive transport network information within the MaaS ecosystem.

Another research deals with the impact of mobility dynamics on location privacy within smart mobility systems (de Mattos et al., 2022). This work highlights the limitations of traditional privacy-preserving methods, such as mix zones and geo-indistinguishability (GEO-I), in dynamic mobility environments.

In the mix zones approach (vodji et al., 2016), designated areas are created where users can temporarily mix or swap their identifiers, disrupting continuous tracking and protecting privacy. However, this method is less effective in highly dynamic settings, like those found in Mobility as a Service (MaaS), where user movement is variable and unpredictable.

Geo-indistinguishability (Elsalamouny and Gambs, 2016), based on differential privacy principles, adds random noise to users' location data, making it challenging to pinpoint their exact position while still enabling approximate location-based services. While useful for static or low-mobility scenarios, geo-indistinguishability can struggle with the dynamic and continuous nature of mobility data in MaaS systems. The study suggests that to enhance both privacy and data utility, privacy mechanisms must be adapted to specific mobility characteristics, advocating for mobility-aware privacy solutions that can dynamically adjust to diverse transport modes and respond to the evolving privacy needs of users in real-time.

Finally, a model addressing the privacy concerns of private transport operators when sharing service tour data with public agencies (He et al., 2017) introduces the "Tour sharing privacy design problem" (TSPDP). This model diffuses actual service tours into a set of possible tours using a probabilistic distribution, maximizing the Shannon Entropy of the flow to maintain a high level of anonymity.

4.3.2. Federated learning architectures

The integration of federated learning architectures (Li et al., 2020) in MaaS systems has emerged as a pivotal approach to enhancing data privacy while maintaining system efficiency and personalization. For instance, the FranchetAI project, as discussed in Pina et al. (2023), highlights the importance of federated learning in promoting sustainable travel behaviors while ensuring user data remains secure. More precisely, by processing data locally on users' devices and employing differential privacy techniques, the project minimizes the risks associated with centralized data storage and unauthorized access, thereby protecting user identities.

Building on this, Chu and Guo (2024) proposes an advanced federated architecture using the federated deep deterministic policy gradient (FDDPG) algorithm. This algorithm combines federated learning principles with Deep Deterministic Policy Gradient (DDPG) reinforcement learning to optimize decision-making in decentralized MaaS systems. Specifically, the FDDPG algorithm is tailored for continuous action spaces, a common need in applications like route optimization. This architecture not only secures passenger data by processing it locally and sharing only encrypted gradients but also ensures robustness against client dropouts through a secure aggregation protocol. This approach is further complemented by the work of Chu and Guo (2023), who introduce a Federated Dynamic Match-Making Algorithm (FDMMA) which operates in a federated learning framework where each service provider locally processes match-making data to protect sensitive business information. In this setup, each provider's system runs its own match-making algorithm on user data and local operational metrics without sharing raw data externally. The federated setup enables these local models to periodically send encrypted updates, rather than raw data, to a central server, which aggregates the updates to refine a global match-making model. This decentralized approach not only improves privacy by keeping data on local servers but also enables real-time adjustments, making it highly adaptive to dynamic conditions within the MaaS ecosystem. Similarly, the future mobility sensing advisor (FMSA) platform (You et al., 2023), leverages federated learning to maintain user privacy by ensuring that sensitive data remains on local devices while only parameters are shared with the central server.

Addressing the broader privacy and security risks in federated MaaS systems, Callegati et al. (2018) explores the vulnerabilities introduced by the integration of cloud-of-things (CoT) with MaaS. CoT refers to the combination of cloud computing with the Internet of Things (IoT), enabling enhanced interoperability and real-time data processing across devices within MaaS ecosystems. However, this integration brings potential risks, particularly around data security and privacy. To mitigate these risks, the study emphasizes the need for robust countermeasures, including overlay networking architecture and gossip protocols. Overlay networking architecture creates a virtual communication layer that secures data routing, isolating sensitive data flows from potential threats. Gossip protocols, a decentralized data-sharing mechanism, incrementally spread information across the network in a controlled manner, reducing data exposure and enhancing resilience against insider threats by limiting unnecessary access to sensitive data. Finally, Chu et al. (2024) delves into the privacy risks associated with federated AI integration in MaaS platforms. This study underscores the necessity of incorporating differential privacy and secure multi-party computation, to safeguard personal data during AI processing.

4.3.3. Blockchain-based privacy-preserving architectures

One instance of a blockchain-based privacy-preserving architectures within the MaaS leverages a decentralized digital identity management framework utilizing self-sovereign identity (SSI) protocols and digital wallets (Hoess et al., 2024). This system allows users to manage and selectively disclose verifiable credentials (VCs) through secure, peer-to-peer channels, using cryptographic techniques like zero-knowledge proofs (ZKPs) to ensure that only necessary data is shared. The use of decentralized identifiers (DIDs) and public key infrastructure (PKI) further enhances security by eliminating the need for centralized control, thus reducing risks associated with traditional data storage methods.

Another study introduces a blockchain-based MaaS system that decentralizes the management of transportation services to improve transparency and trust (Nguyen et al., 2019). This system employs advanced cryptographic methods, including ZKPs, to validate smart contracts without exposing private data, safeguarding users' personal information while maintaining system efficiency. The challenges of balancing data privacy with the dynamic nature of transportation data are addressed through this decentralized approach, which minimizes risks associated with central data storage.

A blockchain-based privacy-preserving driver monitoring system for the vehicular IoT within MaaS is proposed (Kong et al., 2021). This system uses a permissioned blockchain with a proof-of-stake (PoS) consensus mechanism to securely store and disseminate driver performance records, employing a modified paillier cryptosystem and oblivious transfer (OT) protocol for privacy-preserving data retrieval. The inclusion of pseudonyms and cryptographic techniques further protects the identity and location of drivers, ensuring that sensitive data is shared only with authorized parties.

Expanding the discussion, a multi-layered blockchain framework for smart mobility data markets is proposed, addressing the privacy, security and scalability challenges of MaaS (López and Farooq, 2020). This framework facilitates secure data sharing within a blockchain network, ensuring data ownership, transparency and auditability while defending against cybersecurity threats such as spoofing and message interception.

Another study introduces a blockchain-IoT platform tailored for shared mobility services (Auer et al., 2022). This platform uses permissioned blockchain networks to ensure that only authorized entities can access sensitive data, fostering cooperation among stakeholders through a decentralized and transparent ledger. This integration of IoT devices for real-time data collection and blockchain for secure data management effectively addresses privacy concerns while promoting trust and collaboration within the MaaS ecosystem. Finally, a decentralized community of practice (CoP)-based model for on-demand electric car-pooling is proposed, leveraging distributed ledger technologies (DLT) like hyperledger fabric (Anthony, 2024). This model emphasizes a community-driven approach, in which users can securely and privately exchange data without relying on a central third party. The use of smart contracts within this framework enhances security and transparency, addressing common concerns associated with centralized platforms and advancing the technical capabilities of blockchain in mobility services.

4.3.4. Privacy-preserving optimization techniques

The integration of privacy-preserving optimization techniques within the MaaS ecosystem addresses the balancing of data privacy with operational efficiency. One study Abolo-Sewovi et al. (2023) introduces a novel solution for generating on-demand mobility data in regions in which real mobility data collection is costly or impractical. By simulating individual passenger requests using aggregated urban bus data and publicly available geographical information, this approach enhances the ability to explore and optimize on-demand mobility services while ensuring that privacy is preserved.

Similarly, Pandey et al. (2019) explores the challenges of managing competition and cooperation among ride-sharing companies within MaaS platforms, with a focus on data privacy concerns. The study emphasizes the need for balance in information sharing, in which companies must collaborate to optimize vehicle dispatching and route planning while safeguarding sensitive operational data. By proposing a cooperative model that minimizes data sharing and contrasting centralized with decentralized optimization approaches, the study highlights the potential of privacy-preserving strategies to protect sensitive data while maintaining system efficiency and competitiveness.

Building on these concepts, a privacy-preserving framework for fleet management within MaaS platforms is presented (Belletti and Bayen, 2017). This approach involves optimizing on-demand traffic fleet operations through a distributed optimization algorithm that runs on a smartphone-based platform. This method allows drivers to match with ride requests without sharing sensitive data, such as their availability, with the central operator. This scalable, distributed algorithm tackles efficient fleet management while preserving individual drivers' privacy.

Another study Chen et al. (2023) introduces a method for optimizing privacy budget allocation within a differential privacy framework, specifically tailored for public transit trajectory data. By using a prefix tree structure and a Lagrangian relaxation technique, the study tackles

the optimization of the privacy budget allocation across different tree nodes, minimizing query errors while maintaining data utility. The approach, implemented with Shenzhen metro data, showed how to improve the balance between data utility and privacy in smart mobility applications.

Finally, a privacy-preserving matching mechanism called VOting-based MAtching (VOMA) is introduced (Gao et al., 2022). It was designed specifically for community ride-sharing platforms in which users have strong personal preferences. VOMA employs a distributed implementation of the simulated annealing meta-heuristic to achieve near-optimal matching solutions while protecting user privacy. The mechanism achieves high matching efficiency and significant VMT savings. It also addresses scaling in real-world settings, as validated through experiments using New York taxi datasets.

4.4. Privacy perception and regulatory impact

Privacy perceptions and regulatory frameworks play a significant role in the adoption of MaaS systems, though their impact can vary. One study Heering et al. (2023) reveals that while privacy and security concerns are often viewed as barriers to MaaS adoption, they do not significantly deter travelers from using these services. Instead, trust in MaaS providers, particularly regarding the handling of user data, is more influential in user adoption decisions. The study also notes that while personal experiences with privacy invasions have little effect on user intentions, frequent exposure to news about data misuse does influence their decisions, suggesting that cultivating a trustworthy image is important for MaaS providers rather than focusing solely on privacy and security concerns.

Another study Cottrill (2020) emphasizes the importance of regulatory frameworks, particularly the GDPR in the EU, in shaping how MaaS providers manage data privacy. This study underscores the critical role of trust, reliability and transparency in the success of MaaS platforms. It argues that even if end users do not always prioritize privacy issues, the GDPR mandates that MaaS providers implement privacy-by-design (in which privacy is integrated as a fundamental requirement since the design phase of the project), secure user consent and adhere to stringent data protection measures. The analysis of the Whim application's privacy policy (Huang, 2022) illustrates the practical challenges of complying with GDPR while maintaining user trust, highlighting the importance of regulatory compliance in fostering a secure MaaS ecosystem. Whim, developed by MaaS Global, is a mobility-as-a-service application that allows users to plan, book, and pay for various modes of transport—such as public transit, taxis, bike-sharing, and rental cars—all within a single platform. Further exploring the relationship between privacy concerns and MaaS adoption, the study Huang (2022) highlights that while privacy concerns exist, they are not the dominant factor influencing users' decisions to use MaaS. Instead, trust in service providers plays a more critical role. The study also reveals that different user groups exhibit varying levels of privacy concerns, with younger users and those with lower educational backgrounds showing less concern. It confirms the "privacy paradox", in which users express concerns about privacy but do not let these concerns significantly impact their adoption of the service. Thus, building and maintaining trust may be more crucial than solely addressing privacy concerns to encourage broader MaaS adoption.

From a regulatory perspective, establishing robust data protection mechanisms compliant with regulations like the GDPR is essential. One study Williams (2021) highlights the pivotal role of a broker in implementing privacy safeguards, acting as a custodian of user data to ensure it is handled securely and in compliance with privacy regulations. The study also discusses the importance of a solid governance model to clearly define responsibilities and processes related to data management and privacy protection, providing insights into how privacy can be effectively managed in a complex multi-stakeholder MaaS environment.

Another study Pagoni et al. (2022) investigates the broader regulatory and operational challenges faced by MaaS implementation across Europe, highlighting the need for a supportive policy framework that addresses privacy concerns as well as technical, financial, and social barriers. By reviewing existing European regulations and gathering qualitative data from key stakeholders, the study identifies critical enablers and barriers that must be addressed to achieve seamless MaaS integration. The research underscores the importance of clear and consistent regulatory policies to facilitate collaboration among public authorities, MaaS operators, and other stakeholders, ensuring that privacy is protected while promoting the sustainability of MaaS systems.

According to Jittrapirom et al. (2018), the dynamic adaptive policymaking (DAP) approach is introduced as an iterative and flexible strategy to manage uncertainties in implementing MaaS. DAP involves creating an adaptable policy framework that is continuously monitored through key indicators to detect when adjustments are needed. This approach categorizes uncertainties into levels and uses various actions, such as shaping, hedging, and mitigating, to address potential vulnerabilities. In the context of MaaS, DAP helps policymakers navigate challenges like data privacy concerns and stakeholder collaboration by allowing for dynamic policy adjustments as new conditions arise.

Finally, according to Hunecke et al. (2021), data misuse acts as a significant psychological barrier to adopting peer-to-peer collaborative car use within the MaaS ecosystem. The study reveals that concerns over improper access, sharing, or exploitation of personal information markedly reduce users' willingness to participate in such services. This underscores the need for robust data protection mechanisms and transparent privacy policies to foster trust among users, facilitating broader adoption of peer-to-peer car-sharing services, which is crucial in the design and implementation of these platforms.

5. Discussion

5.1. Summary of main findings

The current study systematically investigated literature relevant to data privacy in MaaS from the scope of historical trends, research areas, main topics and key findings. In general, there is a growing interest in research on this topic, although the number of focused articles remains somewhat limited but is increasing as the MaaS ecosystem continues to develop. This investigation specifically responds to the research questions by examining the predominant data privacy challenges within the MaaS ecosystem, the privacy-preserving technologies addressing these challenges and the role of regulatory frameworks in shaping data privacy practices.

Notably, the main journals and conferences in transportation and related fields showed a similar trend of scarcity in dedicated studies on MaaS data privacy. For instance, high-impact journals such as IEEE Transactions on Intelligent Transportation Systems and Transportation Research Part C: Emerging Technologies have published a few articles directly addressing these privacy concerns (Chu and Guo, 2024; López and Farooq, 2020). This scarcity highlights one of the predominant challenges identified in the research question: a need for more extensive investigation into privacy-related issues within MaaS, given the rapid growth of this sector. Additionally, the integration of privacy considerations into transportation policies, as observed in journals like Transportation Research Part A: Policy and Practice, remains underexplored, signaling a gap between technological advancements and their regulatory implications (Cottrill, 2020).

Moreover, the representation of privacy-focused research in conferences such as the IEEE International Conference on Intelligent Transportation Systems and Transportation Research Procedia also highlights the growing but still limited attention given to this critical issue (Chu and Guo, 2023). Despite the increasing relevance of data privacy in the

context of smart mobility, these forums often prioritize broader technological innovations over the nuanced challenges of privacy protection. This finding directly addresses the first research question by identifying the key privacy challenges, notably the underrepresentation of privacy concerns in the broader discourse on MaaS technologies.

The distribution of research across various academic disciplines further illustrates the evolving nature of this field. For instance, the dominance of transportation-related studies suggests that the primary focus has been on the operational and technological aspects of MaaS, while areas like business, economics and policy have received comparatively less attention. This emphasizes the need for a multidisciplinary approach to data privacy, aligning with the second research question regarding the role of regulatory frameworks in shaping privacy practices. The analysis underscores the need for more comprehensive and interdisciplinary approaches to study data privacy in MaaS, bridging the gaps between technology, policy and user trust. As the ecosystem continues to evolve, it is imperative that future research also addresses the broader societal and regulatory challenges associated with data privacy in MaaS.

Despite the growing focus on data privacy in MaaS, legislative frameworks like the *California Consumer Privacy Act* (CCPA) and its amendments under the *California Privacy Rights Act* (CPRA) remain underexplored in the current literature BUKATY (2019). This observation directly answers the second research question regarding the implications of regulatory frameworks on data privacy, noting the gaps in their current exploration and implementation in the MaaS context. While these laws have critical implications for businesses handling personal data, especially in the mobility sector, there is a notable gap in discussing how such regulations impact MaaS platforms. Similarly, Canada's re-evaluation of its *Personal Information Protection and Electronic Documents Act* (PIPEDA) under Bill C-27 has not been sufficiently addressed in terms of its applicability to MaaS systems (of Canada, 2000, 2022). In Québec, the implementation by phases of Bill 25, modernizing personal data protection, introduces stricter obligations for private businesses (Anon, 2023), yet its influence on MaaS operations is still largely unexamined. These gaps indicate a need for further research on the intersection of evolving data protection laws and their practical implications for the development and deployment of MaaS.

The findings from the key themes identified in the systematic review can be broadly categorized into three main areas: Privacy-Preserving Techniques, User Trust and Privacy Perceptions and Regulatory Frameworks. The exploration of privacy-preserving techniques, such as anonymization strategies and encryption methods, responds to the first research question on how privacy-preserving technologies address the identified challenges. Privacy-Preserving Techniques include various methods such as anonymization strategies like k-anonymity and differential privacy (He et al., 2017; He and Chow, 2019; Martelli et al., 2021; Righini et al., 2022; de Mattos et al., 2022; Chevallier et al., 2023), cryptographic approaches including blockchain and encryption protocols (Nguyen et al., 2019; López and Farooq, 2020; Kong et al., 2021; Auer et al., 2022; Anthony, 2024; Hoess et al., 2024), federated learning for decentralized data processing (Callegati et al., 2018; Chu and Guo, 2023; Pina et al., 2023; Chang and Lin, 2023; You et al., 2023; Chu et al., 2024), and advanced algorithms for optimizing privacy budget and utility-privacy trade-offs (Belletti and Bayen, 2017; Pandey et al., 2019; Gao et al., 2022; Abolo-Sewovi et al., 2023; Chen et al., 2023). These techniques are crucial in addressing the complex challenges of data privacy in MaaS, offering scalable and secure solutions that balance privacy with operational efficiency.

User trust and privacy perceptions are also central to the adoption and success of MaaS systems. Trust in service providers is critical, as users need assurance that their data will be handled securely and transparently. This directly relates to both research questions, as it shows how regulatory frameworks and privacy technologies affect user trust, an essential factor for the successful adoption of MaaS systems. Privacy concerns can influence adoption, but the privacy paradox highlights that users often continue to use data-sharing services despite expressing privacy concerns. Awareness of data misuse also plays a significant role in shaping user trust and, consequently, the adoption of MaaS. Compliance with Regulatory Frameworks, such as GDPR, is essential for ensuring strict data protection and embedding privacy considerations into the system architecture from the outset. These frameworks respond to the second research question, demonstrating how they shape privacy practices in MaaS ecosystems. They not only protect user data but also help build trust and ensure that MaaS systems are compliant with evolving legal requirements (Heering et al., 2023; Cottrill, 2020; Huang, 2022; Williams, 2021; Pagoni et al., 2022; Jittrapirom et al., 2018; Hunecke et al., 2021).

5.2. Relationship with other existing surveys

While this review focuses privacy concerns, it stands in contrast to broader examinations of MaaS challenges. For instance, Butler et al. (2021) explores the wide-ranging risks and barriers associated with MaaS adoption, such as public–private cooperation, service coverage, and user acceptance, which could impede the realization of MaaS benefits. Complementing this perspective, Arias-Molinares and García-Palomares (2020) provides a foundational overview of MaaS, examining its key dimensions – what, when, where, who, how, and why – and tracing the concept's evolution. Meanwhile, Kayikci and Kabadurmus (2022) narrows the focus to the specific barriers to MaaS adoption in Istanbul, an emerging metropolis, emphasizing the unique legal, infrastructural, and socio-economic challenges that could affect MaaS implementation. Adding to this discourse, Mustapha et al. (2024) investigates the factors influencing user acceptance of MaaS through empirical studies, while Utriainen and Pöllänen (2018) offers a comprehensive review of the development, concepts, and trends in MaaS literature, encapsulating the breadth of research in this field. Similarly, Kriswardhana and Esztergár-Kiss (2023) provides a systematic literature review focusing on the socio-technical factors influencing the adoption of MaaS and the creation of mobility packages, further contributing to the broader understanding of MaaS adoption.

5.3. Future research directions and research gaps

While significant advancements have been made in the research on MaaS, several areas require further exploration to fully secure and optimize these systems. One of the most pressing concerns that remains insufficiently addressed is the balance between enhancing service operations through data sharing and protecting user privacy. Although privacy-preserving technologies have advanced, there is a research gap in understanding how to integrate these solutions with legal, economic and managerial frameworks, which are essential for a more interdisciplinary approach. Future research should aim to develop frameworks that facilitate the secure exchange of data among stakeholders while minimizing privacy risks (Ekpo et al., 2024). This endeavor involves investigating novel cryptographic methods and privacy-preserving technologies capable of enabling data sharing without compromising user confidentiality. However, the scalability and real-world application of such methods, like blockchain and federated learning, are underexplored, and further work is needed to ensure these technologies can be applied efficiently on a large scale. Additionally, it is crucial to evaluate the impact of these frameworks on user trust and adoption, ensuring that privacy measures align with user expectations and regulatory mandates. There is a gap in understanding how privacy perceptions vary across different user demographics and regions, as well as how the "privacy paradox" (in which users express concerns but still share data) affects adoption rates. The implementation of Privacy Impact Assessments (PIAs) could further help in identifying and mitigating privacy risks throughout the lifecycle of MaaS systems, as outlined in Fig. 6, which illustrates a structured approach to PIAs across the MaaS ecosystem (Wairimu et al., 2024).

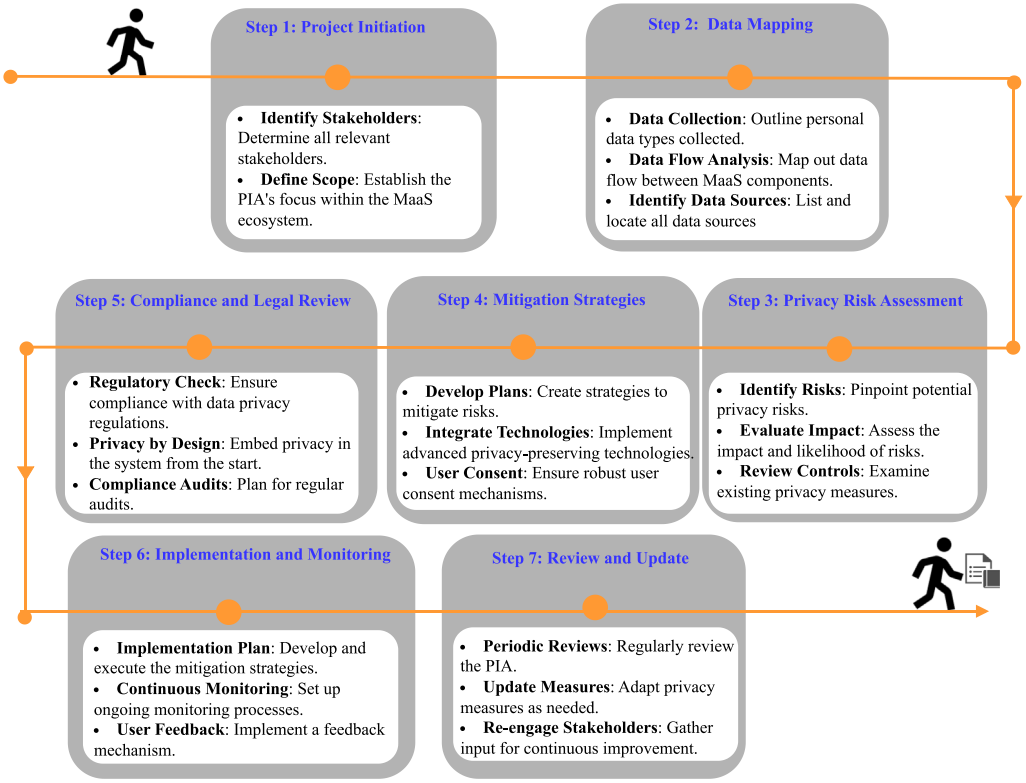


Fig. 6. PIA for data privacy in MaaS.

As MaaS platforms continue to integrate diverse transportation services, the need for secure and seamless interoperability among these services becomes increasingly critical. Research should focus on exploring secure authentication mechanisms that function efficiently across different platforms while upholding high standards of privacy. This includes examining the potential of decentralized identity management systems, which could reduce reliance on single intermediaries and, consequently, mitigate risks associated with centralized data storage and processing. However, current research often overlooks the development of holistic privacy frameworks that encompass all stages of data collection, processing and sharing, highlighting another critical research gap. The importance of interoperability in facilitating such integrations is well-documented, particularly in the context of mobility on demand, in which consistent data structures and open-source standards play a vital role (Kummetha et al., 2024).

Given the growing complexity of MaaS platforms, there is a heightened demand for privacy-preserving solutions that are not only secure but also computationally efficient. Future studies should aim at developing algorithms that provide robust privacy protection with minimal computational overhead. This is particularly relevant for cloud computing contexts, in which current privacy-preserving methods may compromise system performance, especially with respect to matching accuracy and real-time responsiveness. Research should prioritize optimizing these techniques to ensure they maintain both privacy and system performance.

With the evolution of regulatory landscapes, particularly the enforcement of stringent data protection laws like the GDPR, CCPA, Canada's Bill C-27 and Québec's Bill 25, MaaS platforms must be designed to comply with these regulations while remaining adaptable to future changes. Bill C-27, which aims to modernize Canada's privacy legislation under the Digital Charter Implementation Act, introduces stricter consent requirements, data portability and the right to deletion. In Québec, Bill 25 modernizes privacy protections by implementing new obligations for businesses, such as appointing a privacy officer and reporting data breaches. Further research is required to develop privacy frameworks that are responsive to these regulatory requirements and capable of evolving with the legal landscape.

Regulatory and governance models, particularly ones that balance the privacy concerns of various stakeholders, are underdeveloped, revealing another research gap. This includes exploring the role of PIA in the design and implementation of MaaS systems to ensure that privacy considerations are integrated from the outset. Each MaaS project should follow a standardized PIA process to systematically identify risks, develop mitigation strategies and ensure compliance with regulatory obligations. However, the literature often overlooks how PIAs can be continuously updated to reflect evolving privacy laws and technologies. Thus, more emphasis is needed on how PIAs can be embedded as a continuous and adaptive process rather than a one-time activity, ensuring long-term compliance and user trust (Wairimu et al., 2024).

The MaaS ecosystem involves a multitude of actors, including service providers, users and regulatory bodies, each with distinct privacy concerns and operational goals. Future research should also explore strategies to foster cooperation and collaboration among these stakeholders, ensuring that privacy is maintained across the entire ecosystem. This includes addressing the research gap on developing governance models that facilitate collaboration while balancing the competing interests of different actors (Mladenović and Haavisto, 2021).

Finally, there is an increasing recognition of the importance of embedding privacy considerations into the design of MaaS platforms from the very beginning. Future studies should explore how privacy-by-design principles can be effectively integrated into the development lifecycle of MaaS systems. Although privacy-by-design is widely advocated, its practical implementation in MaaS platforms remains insufficiently researched, presenting another key gap. This includes investigating the role of privacy impact assessments and other proactive privacy measures in the design, implementation and operation of MaaS platforms. Exploring these open research areas and gaps will enable future studies to contribute to the creation of more secure, efficient and user-friendly MaaS platforms, ultimately enhancing the sustainability and success of urban mobility systems (Daou and Leurent, 2024; Mladenović and Haavisto, 2021).

5.4. Limitations

This systematic review has several limitations that may affect its scope and comprehensiveness. Despite using a broad search string to capture various terminologies related to MaaS and data privacy, the reliance on specific keywords in titles, abstracts and keywords may have led to the exclusion of relevant studies that did not explicitly mention these terms. Although we also reviewed the references of each selected paper to identify potentially omitted studies, some relevant papers may still have been missed. Additionally, the search was limited to English-language publications, potentially introducing language bias and missing valuable research published in other languages. The term "Mobility as a Service" is used inconsistently across different disciplines and industries, which is why our search strategy included various synonyms and related terms such as "On-Demand Mobility", "Shared Mobility" as well as "Smart Mobility". However, even with this approach, there is no guarantee that all relevant studies were captured. The review's emphasis on certain aspects of MaaS, such as privacy-preserving technologies, might have overlooked other critical areas like user consent and data ownership. Furthermore, the temporal limitation to studies published between 2000 and August 14, 2024 may not fully capture the most recent advancements in the field. Additionally, the heterogeneity of the included studies, with diverse methodologies and research contexts, posed challenges in synthesizing findings, which may have impacted the consistency and generalizability of the conclusions drawn. Finally, the review may have underrepresented the perspectives of various stakeholders, limiting the applicability of the findings across different contexts within the MaaS ecosystem.

6. Conclusion

This systematic review has assessed the data privacy challenges in MaaS, focusing on the existing privacy-preserving technologies, regulatory frameworks and user trust. In particular, the review highlighted that while technologies such as federated learning, blockchain, optimization, and anonymization techniques offer promising solutions for safeguarding user data, their implementation across the entire MaaS ecosystem remains fragmented and inconsistent. Regulatory frameworks like the GDPR play a crucial role in shaping privacy practices, but gaps still exist, particularly in addressing the unique complexities of MaaS systems. The findings emphasize the need for a more integrated approach, combining technological advancements with robust governance models and a focus on user-centered design to fully address data privacy concerns in MaaS. This review also identified several underexplored areas, including the development of scalable privacy frameworks and adaptive regulatory mechanisms that can evolve with the rapidly changing MaaS landscape. Addressing these gaps will be key to fostering user trust and ensuring the sustainable growth of MaaS platforms.

CRediT authorship contribution statement

Zineb Garroussi: Writing – review & editing, Writing – original draft, Visualization, Validation, Methodology. **Antoine Legrain:** Writing – review & editing, Validation, Supervision, Methodology. **Sébastien Gambs:** Writing – review & editing, Visualization, Validation, Supervision, Methodology. **Vincent Gautrais:** Writing – review & editing, Supervision, Methodology. **Brunilde Sansò:** Writing – review & editing, Validation, Supervision.

Declaration of Generative AI and AI-assisted technologies in the writing process

During the preparation of this work the authors used OpenAI in order to paraphrase and check grammar and spelling. After using this tool/service, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

We gratefully acknowledge the financial support from FRQNT, Canada, grant number #323365.

Data availability

No data was used for the research described in the article.

References

Abolo-Sewovi, K.R., Lamrous, S.A., Atchonouglo, K., Baala, O., 2023. Generating on-demand mobility data for urban vehicles based on bus aggregated data. In: 2023 IEEE 26th International Conference on Intelligent Transportation Systems. ITSC, pp. 3377–3382. http://dx.doi.org/10.1109/ITSC57777.2023.10422650.

Anon, 2023. Commission d'accès à l'information du Québec. URL https://www.cai.gouv.qc.ca/entreprises/. (Accessed 14 June 2024).

Anthony, B., 2024. Developing a decentralized community of practice-based model for on-demand electric car-pooling towards sustainable shared mobility. Case Stud. Transp. Policy 15, 101136. http://dx.doi.org/10.1016/j.cstp.2023.101136.

Arias-Molinares, D., García-Palomares, J.C., 2020. The Ws of MaaS: Understanding mobility as a service fromaliterature review. IATSS Res. 44 (3), 253–263. http://dx.doi.org/10.1016/j.iatssr.2020.02.001.

Asensio, O.I., Apablaza, C.Z., Lawson, M.C., Chen, E.W., Horner, S.J., 2022. Impacts of micromobility on car displacement with evidence from a natural experiment and geofencing policy. NATURE ENERGY 7 (11), 1100–1108. http://dx.doi.org/10.1038/s41560-022-01135-1.

Athanasopoulou, A., Deijkers, T., Ozkan, B., Turetken, O., 2022. Maas platform features: An exploration of their relationship and importance from supply and demand perspective. J. Urban Mobil. 2, 100028. http://dx.doi.org/10.1016/j.urbmob.2022.100028.

Auer, S., Nagler, S., Mazumdar, S., Mukkamala, R.R., 2022. Towards blockchain-IoT based shared mobility: Car-sharing and leasing as a case study. J. Netw. Comput. Appl. 200, 103316. http://dx.doi.org/10.1016/j.jnca.2021.103316.

Becker, H., Balac, M., Ciari, F., Axhausen, K.W., 2020. Assessing the welfare impacts of shared mobility and mobility as a service (MaaS). Transp. Res. Part A: Policy Pr. 131, 228–243. http://dx.doi.org/10.1016/j.tra.2019.09.027, Developments in Mobility as a Service (MaaS) and Intelligent Mobility.

Belletti, F., Bayen, A.M., 2017. Privacy-preserving maas fleet management. Transp. Res. Procedia 23, 1000–1024. http://dx.doi.org/10.1016/j.trpro.2017.05.055, Papers Selected for the 22nd International Symposium on Transportation and Traffic Theory Chicago, Illinois, USA, 24-26 July, 2017..

BUKATY, P., 2019. The California Consumer Privacy Act (CCPA): An implementation guide. IT Governance Publishing, http://dx.doi.org/10.2307/j.ctvjghvnn.

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, 103036. http://dx.doi.org/10.1016/j.cities.2020.103036.

Callegati, F., Giallorenzo, S., Melis, A., Prandini, M., 2018. Cloud-of-things meets mobility-as-a-service: An insider threat perspective. Comput. Secur. 74, 277–295. http://dx.doi.org/10.1016/j.cose.2017.10.006.

of Canada, G., 2000. Personal information protection and electronic documents act (S.C. 2000, c. 5). URL https://laws-lois.justice.gc.ca/pdf/p-8.6.pdf. (Accessed 10 August 2024).

of Canada, G., 2022. Bill C-27 on an act to enact the consumer privacy protection act, the personal information and data protection tribunal act and the artificial intelligence and data act and to make consequential and related amendments to other acts. URL https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading. (Accessed 28 June 2024).

Casquero, D., Monzon, A., García, M., Martínez, O., 2022. Key elements of mobility apps for improving urban travel patterns: A literature review. Futur. Transp. 2 (1), 1–23. http://dx.doi.org/10.3390/futuretransp2010001.

Chang, Y.-W., Lin, T.-N., 2023. Federated dynamic match-making for co-opetition among participants in mobility-as-a-service. In: 2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom). pp. 617–621. http://dx.doi.org/10.1109/MetaCom57706.2023.00108.

Chen, C., Hu, X., Li, Y., Tang, Q., 2023. Optimization of privacy budget allocation in differential privacy-based public transit trajectory data publishing for smart mobility applications. IEEE Trans. Intell. Transp. Syst. 24 (12), 15158–15168. http://dx.doi.org/10.1109/TITS.2023.3309783.

Chevallier, T., Lauer, J., Renso, C., Blanco-Justicia, A., De Ryck, D., Papacharalampous, A., 2023. Making it easy for transport stakeholders to share mobility data. Transp. Res. Procedia 72, 2237–2244. http://dx.doi.org/10.1016/j.trpro.2023.11.711, TRA Lisbon 2022 Conference Proceedings Transport Research Arena (TRA Lisbon 2022), 14th-17th November 2022, Lisboa, Portugal.

Chris Jay Hoofnagle, B.v.d.S., Borgesius, F.Z., 2019. The European union general data protection regulation: what it is and what it means*. Inf. Commun. Technol. Law 28 (1), 65–98. http://dx.doi.org/10.1080/13600834.2019.1573501.

Chu, K.-F., Guo, W., 2023. Federated reinforcement learning for consumers privacy protection in mobility-as-a-service. In: 2023 IEEE 26th International Conference on Intelligent Transportation Systems. ITSC, pp. 4840–4846. http://dx.doi.org/10.1109/ITSC57777.2023.10422279.

Chu, K.-F., Guo, W., 2024. Privacy-preserving federated deep reinforcement learning for mobility-as-a-service. IEEE TRANSACTIONS INTELLIGENT TRANSPORTATION SYSTEMS 25 (2), 1882–1896. http://dx.doi.org/10.1109/TITS.2023.3317358.

Chu, K.-F., Yuan, H., Yuan, J., Guo, W., Balta-Ozkan, N., Li, S., 2024. A survey of artificial intelligence-related cybersecurity risks and countermeasures in mobility-as-a-service. IEEE Intell. Transp. Syst. Mag. 2–20. http://dx.doi.org/10.1109/MITS.2024.3427655.

Cottrill, C.D., 2020. Maas surveillance: Privacy considerations in mobility as a service. Transp. Res. Part A: Policy Pr. 131, 50–57. http://dx.doi.org/10.1016/j.tra.2019.09.026, Developments in Mobility as a Service (MaaS) and Intelligent Mobility.

Daou, S., Leurent, F., 2024. Modelling mobility as a service: A literature review. Econ. Transp. 39, 100368. http://dx.doi.org/10.1016/j.ecotra.2024.100368.

de Mattos, E.P., Domingues, A.C.S.A., Santos, B.P., Ramos, H.S., Loureiro, A.A.F., 2022. The impact of mobility on location privacy: A perspective on smart mobility. IEEE Syst. J. 16 (4), 5509–5520. http://dx.doi.org/10.1109/JSYST.2022.3147808.

Dwork, C., Roth, A., 2014. The Algorithmic Foundations of Differential Privacy. http://dx.doi.org/10.1561/0400000042.

Ekpo, O., Casola, V., De Benedictis, A., 2024. Security and privacy issues in Mobility-as-a-Service (MaaS): A systematic review. In: 2024 19th Annual System of Systems Engineering Conference (SoSE). pp. 300–307. http://dx.doi.org/10.1109/SOSE62659.2024.10620969.

Elsalamouny, E., Gambs, S., 2016. Differential privacy models for location- based services. Trans. Data Priv. 9, 15–48.

Enoch, M., Potter, S., 2023. MaaS (Mobility as a Service) market futures explored. Transp. Policy 134, 31–40. http://dx.doi.org/10.1016/j.tranpol.2023.02.007.

Gao, J., Wong, T., Selim, B., Wang, C., 2022. VOMA: A privacy-preserving matching mechanism design for community ride-sharing. IEEE Trans. Intell. Transp. Syst. 23 (12), 23963–23975. http://dx.doi.org/10.1109/TITS.2022.3197990.

He, B.Y., Chow, J.Y., 2019. Optimal privacy control for transport network data sharing. Transp. Res. Procedia 38, 792–811. http://dx.doi.org/10.1016/j.trpro.2019.05.041, Journal of Transportation and Traffic Theory.

He, Y., Chow, J.Y.J., Nourinejad, M., 2017. A privacy design problem for sharing transport service tour data. In: 2017 IEEE 20th International Conference on Intelligent Transportation Systems. ITSC, pp. 1–6. http://dx.doi.org/10.1109/ITSC.2017.8317692.

Heering, M.S., Yuan, H., Li, S., 2023. The impact of privacy and security attitudes and concerns of travellers on their willingness to use mobility-as-a-service systems. In: 2023 IEEE 26th International Conference on Intelligent Transportation Systems. ITSC, pp. 5573–5578. http://dx.doi.org/10.1109/ITSC57777.2023.10422468.

Hoess, A., Lautenschlager, J., Sedlmeir, J., Fridgen, G., Schlatt, V., Urbach, N., 2024. Toward seamless mobility-as-a-service. Bus. Inf. Syst. Eng. http://dx.doi.org/10.1007/s12599-024-00856-9.

Huang, S., 2022. Listening to users' personal privacy concerns. The implication of trust and privacy concerns on the user's adoption of a MaaS-pilot. Case Stud. Transp. Policy 10 (4), 2153–2164. http://dx.doi.org/10.1016/j.cstp.2022.09.012.

Hunecke, M., Richter, N., Heppner, H., 2021. Autonomy loss, privacy invasion and data misuse as psychological barriers to peer-to-peer collaborative car use. Transp. Res. Interdiscip. Perspect. 10, 100403. http://dx.doi.org/10.1016/j.trip.2021.100403.

Jittrapirom, P., Marchau, V., van der Heijden, R., Meurs, H., 2018. Dynamic adaptive policymaking for implementing Mobility-as-a Service (MaaS). Res. Transp. Bus. Manag. 27, 46–55. http://dx.doi.org/10.1016/j.rtbm.2018.07.001, Special Issue on Mobility as a Service.

Kayikci, Y., Kabadurmus, O., 2022. Barriers to the adoption of the mobility-as-a-service concept: The case of Istanbul, a large emerging metropolis. Transp. Policy 129, 219–236. http://dx.doi.org/10.1016/j.tranpol.2022.10.015.

Kong, Q., Lu, R., Yin, F., Cui, S., 2021. Blockchain-based privacy-preserving driver monitoring for MaaS in the vehicular IoT. IEEE Trans. Veh. Technol. 70 (4), 3788–3799. http://dx.doi.org/10.1109/TVT.2021.3064834.

Kriswardhana, W., Esztergár-Kiss, D., 2023. A systematic literature review of mobility as a service: Examining the socio-technical factors in MaaS adoption and bundling packages. Travel. Behav. Soc. 31, 232–243. http://dx.doi.org/10.1016/j.tbs.2022.12.007.

Kummetha, V.C., Concas, S., Staes, L., Godfrey, J., 2024. Mobility on demand in the United States – current state of integration and policy considerations for improved interoperability. Travel. Behav. Soc. 37, 100867. http://dx.doi.org/10.1016/j.tbs.2024.100867.

Li, T., Sahu, A.K., Talwalkar, A., Smith, V., 2020. Federated learning: Challenges, methods, and future directions. IEEE Signal Process. Mag. 37 (3), 50–60. http://dx.doi.org/10.1109/MSP.2020.2975749.

López, D., Farooq, B., 2020. A multi-layered blockchain framework for smart mobility data-markets. Transp. Res. Part C: Emerg. Technol. 111, 588–615. http://dx.doi.org/10.1016/j.trc.2020.01.002.

Lund, E., Kerttu, J., Koglin, T., 2017. Drivers and Barriers for Integrated Mobility Services. Tech. rep, K2 Sweden National Centre for Research and Education on Public Transport, http://dx.doi.org/10.13140/RG.2.2.14619.26403.

Martelli, F., Renda, M.E., Zhao, J., 2021. The price of privacy control in mobility sharing. J. Urban Technol. 28 (1-2, SI), 237–262. http://dx.doi.org/10.1080/10630732.2020.1794712.

Mladenović, M.N., Haavisto, N., 2021. Interpretative flexibility and conflicts in the emergence of mobility as a service: Finnish public sector actor perspectives. Case Stud. Transp. Policy 9 (2), 851–859. http://dx.doi.org/10.1016/j.cstp.2021.04.005.

Moher, D., Liberati, A., Tetzlaff, J., Altman, D.G., Group, T.P., 2009. Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. PLoS Med. 6 (7), e1000097. http://dx.doi.org/10.1371/journal.pmed.1000097.

Mustapha, H.E., Ozkan, B., Turetken, O., 2024. Acceptance of mobility-as-a-service: Insights from empirical studies on influential factors. Commun. Transp. Res. 4, 100119. http://dx.doi.org/10.1016/j.commtr.2024.100119.

Nasser, M., 2020. Cochrane handbook for systematic reviews of interventions. AMERICAN JOURNAL PUBLIC HEALTH 110 (6), 753–754. http://dx.doi.org/10.2105/AJPH.2020.305609.

Nguyen, T.H., Partala, J., Pirttikangas, S., 2019. Blockchain-based mobility-as-a-service. In: 2019 28th International Conference on Computer Communication and Networks. ICCCN, pp. 1–6. http://dx.doi.org/10.1109/ICCCN.2019.8847027.

Pagoni, I., Gatto, M., Tsouros, I., Tsirimpa, A., Polydoropoulou, A., Galli, G., Stefanelli, T., 2022. Mobility-as-a-service: insights to policymakers and prospective MaaS operators. Transp. Lett. Int. J. Transp. Res. 14 (4), 356–364. http://dx.doi.org/10.1080/19427867.2020.1815141.

Pandey, V., Monteil, J., Gambella, C., Simonetto, A., 2019. On the needs for MaaS platforms to handle competition in ridesharing mobility. Transp. Res. Part C: Emerg. Technol. 108, 269–288. http://dx.doi.org/10.1016/j.trc.2019.09.021.

Pina, N., Brito, C., Vitorino, R., Cunha, I., 2023. Promoting sustainable and personalised travel behaviours while preserving data privacy. Transp. Res. Procedia 72, 2768–2775. http://dx.doi.org/10.1016/j.trpro.2023.11.819, TRA Lisbon 2022 Conference Proceedings Transport Research Arena (TRA Lisbon 2022), 14th-17th November 2022, Lisboa, Portugal.

Righini, S., Calderoni, L., Maio, D., 2022. A privacy-aware zero interaction smart mobility system. IEEE Access 10, 11924–11937. http://dx.doi.org/10.1109/ACCESS.2022.3146340.

Samarati, P., Sweeney, L., 2018. Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression. http://dx.doi.org/10.1184/R1/6625469.v1, URL https://kilthub.cmu.edu/articles/journal_contribution/Protecting_privacy_when_disclosing_information_k-anonymity_and_its_enforcement_through_generalization_and_suppression/6625469.

Servou, E., Behrendt, F., Horst, M., 2023. Data, AI and governance in MaaS – leading to sustainable mobility? Transp. Res. Interdiscip. Perspect. 19, 100806. http://dx.doi.org/10.1016/j.trip.2023.100806.

Utriainen, R., Pöllänen, M., 2018. Review on mobility as a service in scientific publications. Res. Transp. Bus. Manag. 27, 15–23. http://dx.doi.org/10.1016/j.rtbm.2018.10.005, Special Issue on Mobility as a Service.

vodji, U.M.A., Gambs, S., Huguet, M.-J., Killijian, M.-O., 2016. Meeting points in ridesharing: A privacy-preserving approach. Transp. Res. Part C: Emerg. Technol. 72, 239–253. http://dx.doi.org/10.1016/j.trc.2016.09.017, URL https://www.sciencedirect.com/science/article/pii/S0968090X1630184X.

Wairimu, S., Iwaya, L.H., Fritsch, L., Lindskog, S., 2024. On the evaluation of privacy impact assessment and privacy risk assessment methodologies: A systematic literature review. IEEE Access 12, 19625–19650. http://dx.doi.org/10.1109/ACCESS.2024.3360864.

Williams, B., 2021. Potential solutions to overcoming barriers to MaaS. In: Automated Vehicles and MaaS: Removing the Barriers. IEEE, pp. 185–198. http://dx.doi.org/10.1002/9781119765394.ch9.

You, L., Danaf, M., Zhao, F., Guan, J., Azevedo, C.L., Atasoy, B., Ben-Akiva, M., 2023. A federated platform enabling a systematic collaboration among devices, data and functions for smart mobility. IEEE Trans. Intell. Transp. Syst. 24 (4), 4060–4074. http://dx.doi.org/10.1109/TITS.2023.3236991.