# The Impact of Privacy and Security Attitudes and Concerns of Travellers on Their Willingness to Use Mobility-as-a-Service Systems

Maria Sophia Heering, Haiyue Yuan, Shujun Li
Institute of Cyber Security for Society (iCSS) & School of Computing, University of Kent, UK
{m.s.heering, h.yuan-221, s.j.li}@kent.ac.uk

***Abstract*— This paper reports results from an online survey on the impact of travellers' privacy and security attitudes and concerns on their willingness to use mobility-as-a-service (MaaS) systems. This study is part of a larger project that aims at investigating barriers to potential MaaS uptake. The online survey was designed to cover data privacy and security attitudes and concerns as well as a variety of socio-psychological and socio-demographic variables associated with travellers' intentions to use MaaS systems. The study involved $n = 320$ UK participants recruited via the Prolific survey platform. Overall, correlation analysis and a multiple regression model indicated that, neither attitudes nor concerns of participants over the privacy and security of personal data would significantly impact their decisions to use MaaS systems, which was an unexpected result, however, their trust in (commercial and governmental) websites would. Another surprising result is that, having been a victim of improper invasion of privacy did not appear to affect individuals' intentions to use MaaS systems, whereas frequency with which one heard about misuse of personal data did. Implications of the results and future directions are also discussed, e.g., MaaS providers are encouraged to work on improving the trustworthiness of their corporate image.**

## I. Introduction

With a worldwide growing population, increases in urbanisation levels and associated growing concerns for environmental issues, the transport sector finds itself in a crucial position and in need of more modern, environmentally sustainable and efficient solutions. In fact, transport is recognised as one of the sectors with the largest greenhouse gas emissions in many countries and worldwide [1]. Providing more efficient and greener mobility solutions in urban, suburban and rural areas could produce personal benefits for individuals (e.g., long-term reduced costs as a result of not owning any personal vehicles, more travel choices, and a healthier life style) as well as wider benefits for the society and the planet as a whole (e.g., reduced traffic congestion, and greenhouse gas emissions with a consequent lower impact on global warming). The number of empirical and theoretical studies supporting the development of green transport has been rapidly growing with the aim to promote more sustainable societies, improve individuals' quality of life and creating more functional travel solutions.

Mobility-as-a-service (MaaS), a multi-modal transport service which offers passengers with seamless and end-to-end mobility options, appears to be a significant step in the direction of more efficient and environmentally friendly transport. MaaS offers an integrated system that allows travellers to plan, book and pay for traditional services, such as public transport, as well as on-demand and shared services (e.g., ride-, bike- and car-share) via a single platform [2], [3]. The development and large-scale uptake of this service is expected to reduce private vehicle usage with consequent positive effects on traffic congestion and air and acoustic pollution [4]. To work efficiently, MaaS requires a complex infrastructure and an efficient digital network of stakeholders [5]. However, even when these are provided, a successful implementation is not automatically guaranteed. In fact, the potential of MaaS largely depends on the willingness of travellers to accept these technologies and to change their travelling behaviours and habits accordingly. In order to successfully implement MaaS, it is thus necessary to explore travellers' attitudes, worries and needs [6], [7]. Among the worries that potential users might have, and which could work as barriers to the adoption of MaaS, are users' concerns over the privacy and security of their personal data [8], [9]. In fact, the complex and integrated system required for MaaS to coordinate multi-modal solutions relies on the integration of diverse transport service providers and related stakeholders (e.g., payment processors), who acquire, exchange and process operational data, mostly in a decentralised manner. The decentralisation and flexibility comes with many security and privacy risks [5], [10], [11].

Previous research has considered the privacy and security of personal data as potential barriers to the implementation of MaaS, which however have been discussed mostly from a system-security perspective [5], [10], [11], [12], [13] or a policy and regulations perspective [3], [12], [14], [15]. As we will discuss in Section II-A, how attitudes and concerns of travellers about the privacy and security of their personal data could affect their willingness to use MaaS systems is still less studied with scarce and inconclusive evidence [6], [7], [9], [16], [17], [18]. We aim to contribute to this literature by looking at several indicators of privacy and security

This is the authors' version of the accepted paper. Please cite this paper as follows: Maria Sophia Heering, Haiyue Yuan and Shujun Li (2023) The Impact of Privacy and Security Attitudes and Concerns of Travellers on Their Willingness to Use Mobility-as-a-Service Systems. *Proceedings of the 2023 IEEE 26th International Conference on Intelligent Transportation Systems* (ITSC 2023), pp. 5573–5578, IEEE, doi: 10.1109/ITSC57777.2023.10422468. For the published version, please visit the publisher's website via the DOI link.

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

perceptions and how these relate to travellers' intention to use MaaS systems. To this end, our survey combines several existing scales on internet privacy and security attitudes and concerns (see Section III). Among the indicators of privacy and security concerns, we also included trust in both commercial and governmental websites [13], which are potentially 'more relatable' indicators. Additionally, we also looked at indicators of personal experiences of internet misuse and familiarity with news about misuse of personal data. Analysing data from our survey (see Section IV), we were able to answer the following research questions:

- **RQ1**: Do cyber security and privacy concerns and attitudes affect travellers' decisions to use MaaS systems?
- **RQ2**: Does having been a victim of perceived improper invasion of privacy have an impact on travellers' decisions to use MaaS systems?
- **RQ3**: Does the frequency with which a traveller has come across news of potential misuse of personal data affect their decisions to use MaaS systems?
- **RQ4**: Does trust in how websites handle users' personal data affect their decisions to use MaaS systems?

This research contributes to the literature by concluding that the role that travellers' internet privacy and security concerns have on their willingness to use MaaS systems is more related to 'trust in the provider' and the frequency with which people have come across news about misuse of personal data. This gives rise to several recommendations for MaaS researchers and providers (see Section V).

## II. Related Work

Privacy and security risks have been recognised as critical aspects of the development of MaaS. Research has looked at both technical and socio-technical security risks. We consider a risk technical if it is more about technologies used in MaaS, e.g., denial-of-service (DoS) attacks, ransomware attack [10], [19], [20], and a risk socio-technical if it is more related to socio-technical factors such as behaviours of travellers, operators of MaaS and other related stakeholders, and policy makers (e.g., data misuse through profiling and inference, 'unruly' third-party access and industrial espionage). Although the importance that privacy and security risks have in the development of MaaS has been acknowledged, there is still insufficient research considering the role that travellers' privacy and security attitudes and concerns have on their willingness to use MaaS systems [6], [7], [9], [16], [17], [18]. In fact, while some studies concluded that privacy and security concerns could negatively affect travellers' decisions to adopt MaaS [9], [7], some found that these concerns had no impact [6], [17] and others reported mixed results [16], [17]. Furthermore, past studies have seldom considered the role played by trust in the providers [2], [21], [22] and, to the best of our knowledge, no study has simultaneously measured the impact of privacy and security attitudes/concerns and trust in the providers on travellers' willingness to use MaaS systems. Our work therefore fills this gap, in addition to also looking at two other factors (having been a victim of information misuse and the frequency with which one has heard of information misuse) that may affect travellers' decisions to use MaaS systems.

### A. Privacy and Security Concerns

Privacy and security concerns and risks associated with MaaS systems are closely related to the types of personal data collected and how the collected personal data are used and shared. A number of studies have looked into how personal data collected by MaaS systems can be explored to infer user's behaviour and mobility patterns [23], [24]. For instance, MaaS users' movement data can be analysed to infer information about certain health conditions [24]; location data with information about time of use can be monetised by companies, introducing potential privacy and ethical concerns [25]; a driver's performance data and GPS coordinates can reveal sensitive information, leading to violations of their identity and location privacy [26], [12]. Privacy concerns in MaaS systems extend beyond profiling and inference risks to include third-party access to personal data and over-sharing of personal data between multiple parties. Different stakeholders require access to and processing of personal data for a MaaS system to function effectively. It is essential to examine third-party processors such as payment processors and hosting providers to address privacy considerations and implications [27]. It is also important to understand what data are necessary for what operations and what data are requested unnecessarily by stakeholders [28]. Similarly, some research recommended that users should be given a certain degree of privacy control when their personal data are shared on open data platforms, with the consensus that personal data types and formats can be shared to promote the smooth operation of mobility platforms [29]. To overcome these obstacles, it was highlighted in a previous study that privacy regulations should be carefully considered for supporting the development of MaaS and for enhancing trust of both users and providers [8].

### B. Trust

Trust has been argued to be an important prerequisite for successful e-commerce and e-services. This is because online transactions occur with a high degree of uncertainty (admittedly higher than in face-to-face exchanges) with transactions being blind, borderless and non-instantaneous, online users need to trust the sellers and providers that they will fulfil their obligations without engaging in harmful behaviours (e.g., providing inaccurate information, violating the customers' privacy, and making unauthorised use of credit card information) [30], [31]. A multitude of studies have indeed shown that trust plays an essential role in online transactions, both directly and indirectly through the reduction of consumers' perceived risk [30], [31], [32].

Although trust of travellers has been widely considered as having a crucial role in the implementation of MaaS systems [8], [21], its impact on travellers' willingness to use MaaS systems has been seldom studied. This is surprising considering the following aspects: a) there is a vast literature

on the role that trust plays on consumers' acceptance of e-sellers and e-services, b) research on MaaS has shown that trust in the MaaS providers is positively associated with intentions to purchase MaaS bundles [22], and c) research on MaaS has shown that individuals would wish for the government (admittedly a respectful and trustful stakeholder) to play an active role in the service (both as an overseer or a provider) [2], [21], [22]. We consider the low number of studies assessing and measuring the impact that trust in the MaaS providers and its impact on travellers' intention to use MaaS as an important gap in the literature. More specifically, we feel the need to concurrently measure users' trust in how the provider handles their personal data and their privacy and security concerns. In fact, we believe that trust could be a useful proxy for privacy and security concerns, as it being potentially more familiar and relatable for most non-expert users with less knowledge on privacy and security matters.

## III. Methodology

### A. Procedures and Materials

There are a number of past studies that investigated the impact of privacy and security attitudes and concerns on people's willingness to use MaaS systems. However, such studies are often fragmented and did not systematically consider different aspects of MaaS systems from end users' perspectives. We conducted a large-scale online survey, aiming to comprehensively learn about travellers' security and privacy attitudes in relation to their willingness to use MaaS systems. We included several existing scales on internet privacy and security attitudes and concerns in order to test their potentially different impact on travellers willingness to adopt MaaS. In line with the gaps identified (see Section II-B) we also included measures of trust in commercial and governmental websites. Additionally, because trust in and reputation of a provider can be affected by social-environment cues like media stories of hacking and loss of credit card details [33], we decided to measure how much participants had heard/read about the use of potential misuse of information collected on the Internet and assess whether this would impact the decision to use MaaS systems. Based on previous literature we expected familiarity with information misuse to negatively affect the willingness to use MaaS [33] and for personal experiences of information misuse to do the same. The survey also included a variety of socio-psychological and travel-behaviour related variables that will be discussed in a follow-up paper. The online survey was designed to consist of the following six parts.

- Part 1 contains socio-demographic questions.
- Part 2 focuses on *transport and travel route information behaviour*. Participants were asked questions about their transport and travel information habits (e.g., what trip and route information apps they use and how often they use such apps).
- Part 3 focuses on *data sharing*. Participants were asked questions on how they feel about sharing personal data online (i.e., internet privacy concerns) and on how much they trust or are concerned with the way commercial and governmental websites dispose of users' personal data.
- Part 4 primarily investigates *perceptions about MaaS systems*. Participants were presented with a brief description of MaaS and were subsequently asked how they felt about the service (e.g., perceived usefulness of MaaS, intention to use MaaS if it were available, perceived incentives to use MaaS).
- Part 5 looks at *transportation habits and evaluations*. Participants were asked questions aimed at exploring their personal transport habits and their experiences and impressions of their local public transport systems (e.g., what is their primary mode of transportation, their level of satisfaction with local buses).
- Part 6 is included to learn about how often if ever participants had became a victim of improper invasion of privacy online and how often if ever they had heard about news on misuse of personal data.

After the above six parts, participants were invited to provide any further comments, thanked and debriefed.

This study received a favourable ethical opinion from the Central Research Ethics Advisory Group of the University of Kent (Reference Number: CREAG109-09-22). We used the Jisc Online Surveys system[1] to host the online survey and the crowdsourcing platform Prolific[2] to recruit participants. All participants gave their consent electronically as part of the online survey before proceeding to take the online survey. The participants were compensated financially at a rate of £9 per hour and the survey took an average participant 17 minutes to complete. We carried out a power analysis using G*Power [34], suggesting that a sample size of at least 274 participants is needed to detect a small-to-medium effect size, $f = .17$, at 80% power ($\alpha = .05$). To be on the side of caution, we decided to recruit 320 participants.

### B. Measures

It is worth noting that the emphasis of this paper is on data privacy and security concerns of MaaS, we hereby focus on investigating 1) variables from Part 3 of the survey on data sharing and their relationships with the behavioural intention to use MaaS systems; and 2) variables from Part 6 of our survey, relative to experiences of invasion of privacy and news of information misuse. Variables from the remaining parts of the survey (parts 1, 4 and 5) will be analysed in a follow-up paper. We computed bi-variate correlations to identify which of our variables were significantly associated with the'behavioural intention to use MaaS'. We then used a multiple regression analysis, with 'behavioural intention to use MaaS' as our primary dependent variable (DV), to identify which of those variables would work as a significant predictor (IVs) of the DV. More details about all variables used in this study are presented as follows.

*1) DV: Behavioural Intention to Use MaaS (BIUM):* The intention to use MaaS was measured by asking participants

[1] https://www.onlinesurveys.ac.uk/
[2] https://www.prolific.co/

to indicate how much they disagreed or agreed with the following statements using a 7-point Likert scale (1 = strongly disagree, 7 = strongly agree; $\alpha = .97$):

- '*Assuming I would have access to the MaaS offering, I intend to use it.*'
- '*I expect to use the MaaS offering when it becomes available.*'
- '*Given that I would have access to the MaaS offering, I predict using it.*'

*2) IV: Attitudes towards Personal Identifying Information collection (APII):* Participants were asked to indicate how much they disagreed or agreed with seven different statements borrowed from a previous study [18]. Examples of statements are: '*I want a website to disclose how my PII will be used*', '*I am unconcerned when a website uses my PII to customise my browsing experience (R)*' and '*I mind when a website that I visit collects (without my consent) information about my browser configuration*' (1 = strongly disagree, 7 = strongly agree; $\alpha = .84$).

*3) IVs: Internet Privacy Concerns for Commercial Websites (IPCC) & Internet Privacy Concerns for Governmental Websites (IPCG):* To assess participants' internet privacy concerns we asked them about their level of agreement with 18 different statements borrowed from a previous study [12]. Reliability of this scale was very high, respectively $\alpha = .96$ for commercial websites and $\alpha = .97$ for governmental websites. These items refer to six different domains (Collection, Secondary Usage, Errors, Improper Access, Control and Awareness) and are considered separately for *commercial* and *governmental* websites.

*4) IVs: Trusting Beliefs for Commercial Websites (TBC) & Trusting Beliefs for Governmental Websites (TBG):* We asked participants to indicate their level of agreement with four different statements borrowed from a previous study [13], with the purpose of assessing how much individuals believe they can trust *commercial* and *governmental* websites on handling their personal data. Two example statements are:

- '*Commercial/Governmental websites in general would be trustworthy in handling my personal information.*'
- '*Commercial/Governmental websites would fulfil their promises related to my personal information.*'

All these questions are measured using a 7-point Likert scale (1 = strongly disagree, 7 = strongly agree; $\alpha = .93$ for trust related to commercial websites and $\alpha = .95$ for trust related to governmental websites).

*5) IV: Improper Invasion of Privacy (IIP):* Participants were asked one question: '*How frequently have you personally been the victim of what you felt was an improper invasion of privacy?*' (1 = Never, 6 = Frequently).

*6) IV: News of Information Misuse (NIM):* Participants were asked: '*How much have you heard or read during the last year about the use and potential misuse of the information collected from the Internet?*' (1 = Not at all, 7 = Very much).

## IV. Results

320 individuals from the UK (133 females, 183 males, 3 preferred not say, 1 other) took part in this study. The mean age was 39.71 (SD = 11.79). The majority of the participants reported to be White (85.9%), followed by Asian or Asian British (10%), Black/Black British/ African or Caribbean (2.2%), and (0.9%) from mixed or other ethnicity. No participants were excluded or included following data analysis.

### A. Analysis of Correlations

First of all, we looked at the correlations between 'behavioural intentions to use MaaS' (i.e., DV: BIUM) and indexes for data privacy and data security attitudes and concerns. As suggested by the authors who introduced the scales for Internet Privacy Concerns [13], we computed separate indexes for commercial and government websites (i.e., IVs: IPCC & IPCG). As shown in Table I, participants had moderate to high levels of privacy and security concerns on their personal data (IPCC: $M = 5.48$, SD = 1.02; IPCG: $M = 4.25$, SD = 1.37; and APII: $M = 5.44$, SD = 1.05). However, interestingly and somewhat surprisingly (somewhat because evidence in literature is mixed and so far inconclusive), we found that none of these indexes were significantly correlated with participants' intentions to use MaaS (see Table I). This mismatch between the level of concern and the absence of a relationship between the concern and the intention to use MaaS appears to be in line with literature on the 'privacy paradox', which suggests that, although individuals tend to indicate privacy as a primary concern, they reveal personal information for relatively small rewards [35].

Contrastingly, correlations between BIUM and TBC ($r = .24$, $p \leq .001$) and between BIUM and TBG ($r = .18$, $p \leq .001$) are both positive and significant (although weak), indicating that the trust on commercial and government websites to handle personal data plays a role on nudging participants' intention to use MaaS. Additionally, BIUM was also positively correlated with NIM ($r = .15$, $p = .01$), suggesting that participants' intention to use MaaS is associated with the frequency with which participants had heard about information misuse on the internet. Whereas, there is no correlation between BIUM and IIP ($r = .04$, $p = .50$), which reveals that participants' past experiences of personal invasion of privacy does not seem to affect their willingness to use MaaS. This last result may be surprising, since one could reasonably expect that past experiences of personal invasion of privacy would have a negative impact on people's willingness to use other apps in the future. One plausible explanation for the lack of this correlation is related to the distribution of data. People generally believe that they only infrequently have been victims of misuse of information collected from the internet ($M = 2.31$, SD = 1.08), suggesting that it could be difficult to detect a significant relationship. Finally, and coherent with the notion that to higher trust should correspond lower concerns of users, the correlations between the three indicators of privacy

TABLE I

MEANS, STANDARD DEVIATIONS (SD) AND CORRELATIONS AMONG VARIABLES

| Measures | Mean | SD | BIUM | APII | IPCC | IPCG | TBC | TBG | IIP | NIM |
|---|---|---|---|---|---|---|---|---|---|---|
| BIUM | 4.67 | 1.52 | - | -.06 ($p = .27$) | -.03 ($p = .57$) | -.07 ($p = .21$) | .24 ($p \leq .001$) | .18 ($p \leq .001$) | .04 ($p = .50$) | .15 ($p = .008$) |
| APII | 5.44 | 1.05 | | - | .77 ($p = .008$) | .48 ($p = .008$) | -.34 ($p = .008$) | -.24 ($p = .008$) | .33 ($p = .008$) | .27 ($p = .008$) |
| IPCC | 5.48 | 1.02 | | | - | .56 ($p \leq .001$) | -.36 ($p \leq .001$) | -.22 ($p \leq .001$) | .35 ($p \leq .001$) | .30 ($p \leq .001$) |
| IPCG | 4.25 | 1.37 | | | | - | -.29 ($p \leq .001$) | -.55 ($p \leq .001$) | .33 ($p \leq .001$) | .31 ($p \leq .001$) |
| TBC | 3.80 | 1.37 | | | | | - | .52 ($p \leq .001$) | -.25 ($p \leq .001$) | -.12 ($p = .03$) |
| TBG | 4.77 | 1.38 | | | | | | - | -.17 ($p \leq .001$) | -.14 ($p = .01$) |
| IIP | 2.31 | 1.08 | | | | | | | - | .25 ($p \leq .001$) |
| NIM | 4.26 | 1.51 | | | | | | | | - |

and security attitudes/concerns (i.e., APII, IPCC, and IPCG) and trust in commercial/government websites (i.e., TBC and TBG) are all negative and significant (see Table I).

### B. Regression Analysis

By considering the results from the correlation analysis presented in Section IV-A, here we present a multiple linear regression model to investigate the effects of those variables (i.e., TBC, TBG, and NIM) that have significant correlations with BIUM. The fitted regression model was ($p \leq .001$):

$$\text{BIUM} = 2.46 + .23 \times \text{TBC} + .11 \times \text{TBG} + .19 \times \text{NIM}.$$

The overall regression was statistically significant ($R = 0.31$, $F(3, 316) = 11.09$, $p \leq .001$, $R^2 = .095$, $R^2$ Adjusted $= .087$), however, the model only explains a small amount of the variance in the value of intentions to use MaaS (9.5%). Additionally, it was found that, whereas 'trust in commercial websites' (i.e., TBC) ($\beta = 0.20$, $p \leq .001$) and 'frequency of news misuse' (i.e., NIM) ($\beta = 0.11$, $p \leq .001$) significantly predicts 'intentions to use MaaS' (i.e., BIUM), trust in governmental websites' (i.e., TBG) does not ($\beta = 0.10$, $p = 0.11$).

### C. Results and Discussion

Although MaaS has received increasing interest since it was first presented at ITS Europe Congress held in Helsinki, Finland, in June 2014 [36], research investigating the effects of privacy and security concerns on the intentions to use MaaS by travellers, is still scarce and so far inconclusive. We aimed to bring some clarity to this area of research by concurrently measuring users' trust in how the provider handles their personal data and their privacy and security attitudes and concerns. In our study we did not find any relationship between data privacy/security attitudes/concerns and MaaS usage, however, we found that trust, and more specifically trust in a (commercial and governmental) website's handling of users' personal data, does positively predict our participants' intentions to use MaaS. This result is in line with previous research on MaaS, which identified trust in the provider as relevant and a positive predictor of willingness to adopt MaaS [2], [21], [22], and more importantly, this result is in line with a long tradition of research that identifies trust on website as a core positive predictor of people's intentions to use or buy from online service providers.

One limitation of this study is that we measured trust as trust in how general commercial/governmental websites handle users' personal information and not as trust in how a MaaS system would handle users' personal information. However, we argue that because we did not use a stated preference approach (where participants are asked to make decisions in hypothetical choice scenarios) but simply presented participants with a generic definition of a MaaS system, it would have been too artificial to ask participants how much they would trust this hypothetical system. Additionally, because MaaS systems will necessarily be considered as either commercial or governmental (or potentially hybrid) systems, the trust measures we used should be relevant to MaaS as well.

## V. CONCLUSIONS

In this survey-based study, we investigated the role that privacy and security concerns have on travellers' willingness to use MaaS systems. We concurrently (to the best of our know, for the first time in the literature on MaaS) assessed the role played by trust in the providers and the role played by users' privacy and security attitudes and concerns. Additionally, we tested whether having been a victim of improper invasion of privacy and the frequency with which individuals had heard/read of episodes of internet information misuse would affect their willingness to use MaaS. We did not find evidence to show that privacy and security concerns has significant impact on our participants' intention to use MaaS. Contrastingly, we found that trust in how users' data is handled, and more specifically trust in

how commercial and governmental websites handle users' data, does have an (although small) positive impact on participants' intention to use MaaS. These results are in line with the vast literature showing how trust plays a pivotal role in consumers' acceptance of e-sellers and e-services. We would recommend that *research investigating the role that privacy and security concerns have on travellers' willingness to use MaaS should also consider their trust on providers' handling of personal data*. In comparison with privacy and security concerns, trust could in fact be a more relatable concept for potential MaaS users and a clearer predictor.

This work furthers our understanding of the role played by privacy and security concerns on travellers' intention to use MaaS systems and directs the attention towards the significant influence that trust on providers can have on the MaaS usage intention. We suggest that, *as for most online services, in order to increase the number of customers and to decrease users' perceived risks, MaaS providers must work to build a more trusted and reliable image among people*. For example, to decrease users' perceived privacy and security risks, MaaS systems could provide assurance that they comply with a privacy policy that clearly indicates what personal data will be collected and how such collected personal data will be used and shared [30].

## REFERENCES


[1] D. Sulskyte, "Mobility-as-a-service: Concepts and theoretical approach," in *Proceedings of the 2021 IEEE International Conference on Technology and Entrepreneurship*, 2021.

[2] R. G. Casadó, D. Golightly, K. Laing, R. Palacin, and L. Todd, "Children, young people and Mobility as a Service: Opportunities and barriers for future mobility," *Transportation Research Interdisciplinary Perspectives*, vol. 4, pp. 100 107:1–100 107:11, 2020.

[3] H. Liimatainen and M. N. Mladenović, "Developing mobility as a service – user, operator and governance perspectives," *European Transport Research Review*, vol. 13, no. 1, pp. 37:1–37:3, 2021.

[4] J. Eckhardt, A. Lauhkonen, and A. Aapaoja, "Impact assessment of rural PPP MaaS pilots," *European Transport Research Review*, vol. 12, pp. 49:1–49:14, 2020.

[5] M. H. Chinaei, T. Hossein Rashidi, and T. Waller, "Digitally transferable ownership of mobility-as-a-service systems using blockchain and smart contracts," *Transportation Letters*, vol. 15, no. 1, 2022.

[6] J. Schikofsky, T. Dannewald, and M. Kowald, "Exploring motivational mechanisms behind the intention to adopt mobility as a service (MaaS): Insights from Germany," *Transportation Research Part A: Policy and Practice*, vol. 131, pp. 296–312, 2020.

[7] M. J. Alonso-González, S. Hoogendoorn-Lanser, N. van Oort, O. Cats, and S. Hoogendoorn, "Drivers and barriers in adopting Mobility as a Service (MaaS) – a latent class cluster analysis of attitudes," *Transportation Research Part A: Policy and Practice*, vol. 132, pp. 378–401, 2020.

[8] L. Butler, T. Yigitcanlar, and A. Paz, "Barriers and risks of Mobility-as-a-Service (MaaS) adoption in cities: A systematic review of the literature," *Cities*, vol. 109, pp. 103 036:1–103 036:20, 2021.

[9] J. Ye, J. Zheng, and F. Yi, "A study on users' willingness to accept mobility as a service based on UTAUT model," *Technological Forecasting and Social Change*, vol. 157, pp. 120 066:1–120 066:9, 2020.

[10] F. Callegati, S. Giallorenzo, A. Melis, and M. Prandini, "Cloud-of-Things meets Mobility-as-a-Service: An insider threat perspective," *Computers & Security*, vol. 74, pp. 277–295, 2018.

[11] E. Bothos, B. Magoutas, K. Arnaoutaki, and G. Mentzas, "Leveraging blockchain for open mobility-as-a-service ecosystems," in *Proceedings of the 2019 IEEE/WIC/ACM International Conference on Web Intelligence - Companion Volume*. ACM, 2019, pp. 292–296.

[12] Q. Kong, R. Lu, F. Yin, and S. Cui, "Blockchain-based privacy-preserving driver monitoring for MaaS in the vehicular IoT," *IEEE Transactions on Vehicular Technology*, vol. 70, pp. 3788–3799, 2021.

[13] W. Hong and J. Thong, "Internet privacy concerns: An integrated conceptualization and four empirical studies," *MIS Quarterly*, vol. 37, pp. 275–298, 2013.

[14] P. Jittrapirom, V. Marchau, R. van der Heijden, and H. Meurs, "Dynamic adaptive policymaking for implementing Mobility-as-a Service (MaaS)," *Research in Transportation Business & Management*, vol. 27, pp. 46–55, 2018.

[15] M. Audouin and M. Finger, "The development of Mobility-as-a-Service in the helsinki metropolitan area: A multi-level governance analysis," *Research in Transportation Business & Management*, vol. 27, pp. 24–35, 2018.

[16] A. Polydoropoulou, I. Pagoni, and A. Tsirimpa, "Ready for Mobility as a Service? insights from stakeholders and end-users," *Travel Behaviour and Society*, vol. 21, pp. 295–306, 2020.

[17] V. Caiati, S. Rasouli, and H. Timmermans, "Bundling, pricing schemes and extra features preferences for mobility as a service: Sequential portfolio choice experiment," *Transportation Research Part A: Policy and Practice*, vol. 131, pp. 123–148, 2020.

[18] I. Becker, R. Posner, T. Islam, P. Ekblom, H. Borrion, M. Mcguire, and S. Li, "Privacy in transport? exploring perceptions of location privacy through user segmentation," in *Proceedings of the 54th Hawaii International Conference on System Sciences*, 01 2021, pp. 5347–5356.

[19] L. Mouhibbi, M. Elhozmari, and A. Ettalbi, "Sorting and persisting REST and SOAP client for MaaS based architecture," in *Proceedings of the 2018 6th International Conference on Multimedia Computing and Systems*, 2018.

[20] T. Nguyen, J. Partala, and S. Pirttikangas, "Blockchain-based mobility-as-a-service," in *Proceedings of the 2019 28th International Conference on Computer Communication and Networks*, 2019.

[21] S. Jung, H. Kum-Biocca, F. Biocca, S. Hong, M. Shin, and H. Hu, *Evaluating Global Integrated Transportation Application for Mega Event: Role of Trust and Exchanging Personal Information in Mobility as a Service (MaaS)*, 2020, pp. 575–584.

[22] A. Vij, S. Ryan, S. Sampson, and S. Harris, "Consumer preferences for Mobility-as-a-Service (MaaS) in Australia," *Transportation Research Part C: Emerging Technologies*, vol. 117, pp. 102 699:1–102 699:21, 2020.

[23] L. Barreto, A. Amaral, and S. Baltazar, "Urban mobility digitalization: Towards Mobility as a Service (MaaS)," in *Proceedings of the 2018 International Conference on Intelligent Systems*, 2018, pp. 850–855.

[24] F. Costantini, E. Archetti, F. Di Ciommo, and B. Ferencz, "IoT, intelligent transport systems and MaaS (mobility as a service)," *Jusletter IT*, vol. 21, 2019. [Online]. Available: https://air.uniud.it/retrieve/e27ce0c8-7c87-055e-e053-6605fe0a7873/2019%20Abil%20Jusletter%20IT%20IoT%20MaaS.pdf

[25] P. Cooper, T. Tryfonas, T. Crick, and A. Marsh, "Electric vehicle mobility-as-a-service: Exploring the "Tri-Opt" of novel private transport business models," *Journal of Urban Technology*, vol. 26, no. 1, pp. 35–56, 2019.

[26] F. Belletti and A. M. Bayen, "Privacy-preserving MaaS fleet management," *Transportation research procedia*, vol. 23, pp. 1000–1024, 2017.

[27] C. D. Cottrill, "MaaS surveillance: Privacy considerations in mobility as a service," *Transportation Research Part A: Policy and Practice*, vol. 131, pp. 50–57, 2020.

[28] K. Pitera and G. Marinelli, "Autonomous e-mobility as a service," Norwegian University of Science and Technology (NTNU)," Research Report, 2017. [Online]. Available: http://hdl.handle.net/11250/2496952

[29] B. Y. He and J. Y. J. Chow, "Gravity model of passenger and mobility fleet origin–destination patterns with partially observed service data," *Transportation Research Record*, vol. 2675, no. 6, pp. 235–253, 2021.

[30] D. J. Kim, D. L. Ferrin, and H. R. Rao, "A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents," *Decision Support Systems*, vol. 44, no. 2, pp. 544–564, 2008.

[31] D. Gefen, E. Karahanna, and D. Straub, "Trust and TAM in online shopping: An integrated model," *MIS Quarterly*, vol. 27, pp. 51–90, 2003.

[32] S. A. Qalati, E. Galvan Vela, W. Li, S. A. Dakhan, T. Thi Hong Thuy, and S. Mirani, "Effects of perceived service quality, website quality, and reputation on purchase intention: The mediating and moderating

roles of trust and perceived risk in online shopping," *Cogent Business & Management*, vol. 8, pp. 1 869 363:1–1 869 363:20, 2021.

[33] A. Morton, *"All my mates have got it, so it must be okay": Constructing a Richer Understanding of Privacy Concerns—An Exploratory Focus Group Study*, 2014, pp. 259–298.

[34] F. Faul, E. Erdfelder, A.-G. Lang, and A. Buchner, "G*Power 3: A flexible statistical power analysis program for the social, behavior, and biomedical sciences," *Behavior Research Methods Instruments & Computers*, vol. 39, pp. 175–191, 2007.

[35] S. Kokolakis, "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon," *Computers & Security*, vol. 64, pp. 122–134, 2017.

[36] K. Sakai, "MaaS trends and policy-level initiatives in the EU," *IATSS Research*, vol. 43, no. 4, pp. 207–209, 2019.