5-11-2023

EXPLORING THREAT-SPECIFIC PRIVACY ASSURANCES IN THE CONTEXT OF CONNECTED VEHICLE APPLICATIONS

Henrik Lechte
University of Goettingen, henrik.lechte@uni-goettingen.de

Jannes Heinrich Diedrich Menck
University of Goettingen, jannes.menck@uni-goettingen.de

Alexander Stocker
Virtual Vehicle Research Center, alexander.stocker@v2c2.at

Tim-Benjamin Lembcke
University of Goettingen, tim-benjamin.lembcke@uni-goettingen.de

Lutz M. Kolbe
University of Goettingen, lkolbe@uni-goettingen.de

EXPLORING THREAT-SPECIFIC PRIVACY ASSURANCES IN THE CONTEXT OF CONNECTED VEHICLE APPLICATIONS

Research Paper

Henrik Lechte, University of Goettingen, Germany, henrik.lechte@uni-goettingen.de.

Jannes Heinrich Diedrich Menck, University of Goettingen, Germany, jannes.menck@uni-goettingen.de.

Alexander Stocker, Virtual Vehicle Research GmbH, Austria, alexander.stocker@v2c2.at.

Tim-Benjamin Lembcke, University of Goettingen, Germany, tim-benjamin.lembcke@uni-goettingen.de.

Lutz M. Kolbe, University of Goettingen, Germany, lkolbe@uni-goettingen.de.

Abstract

Connected vehicles enable a wide range of use cases, often facilitated by smartphone apps and involving extensive processing of driving-related data. Since sensitive information about actual driving behavior or even daily routines can be derived from this data, the issue of privacy arises. We explore the impact of short privacy assurance statements on user perceptions by considering two data-intensive cases, usage-based insurance, and traffic hazard warnings. We conducted two experimental comparisons to investigate whether and how privacy-related perceptions about vehicle data sharing can be altered by different text-based privacy assurances on fictional app store pages. Our results are largely inconclusive, and we found no clear evidence that such short statements can significantly alter privacy concerns and increase download intentions. Furthermore, our results suggest that general and threat-specific privacy assurance statements likely yield no or little benefits to connected vehicle app providers regarding user perceptions.

Keywords: Connected vehicles, Privacy assurances, Mobile applications.

1 Introduction

Leveraging digital services in connected vehicles has become essential in changing the driving experience (Athanasopoulou et al., 2016; Bohnsack et al., 2021). Nowadays, modern vehicles collect a wealth of data about themselves and their environment (Stocker et al., 2017; Swan, 2015). Driven by this paradigm, many data-intensive use cases are emerging, ranging from autonomous driving (e.g., Faisal et al., 2019) to predictive maintenance (e.g., Dhall and Solanki, 2017). Smartphone applications are integral to many connected car use cases (Coppola and Morisio, 2016), offering benefits such as low-cost, vehicle-agnostic solutions and the ability to retrofit older vehicles with connected services (Engelbrecht et al., 2015; Seter et al., 2021). These mobile applications, which typically build on vehicle-generated data or track vehicle movements using smartphone sensors (Wahlström et al., 2017), can spawn many use cases such as traffic hazards warnings (Aghayari et al., 2021; Trager et al., 2021), eco-driving (Tulusan et al., 2012), insurance telematics (Händel et al., 2014), and anti-theft tracking (Shruthi et al., 2015). In addition, some apps may use external hardware which can be integrated into different vehicle models, such as OBD2-dongles (e.g., Amarasinghe et al., 2015). Building on this

potentially vast amount of data, applications based on vehicle data are further driven by Artificial Intelligence (e.g., Merenda et al., 2021; Moon et al., 2017; Reddy and Premamayudu, 2019).

For smartphone-enabled applications that process driving-related data, user perceptions and acceptance are often crucial for widespread adoption (Engelbrecht et al., 2015; Mantouka et al., 2021). In this context, information privacy and security are relevant research topics for connected vehicle applications, both from a technical viewpoint (Joy and Gerla, 2015) and a user acceptance perspective (Cichy et al., 2021; Kaiser et al., 2018; Pumplun et al., 2021). Information privacy is particularly relevant for connected cars because of their relationship to the Internet of Things, with continuous data flows often with little control for the user (Cichy et al., 2021). In addition, driving-related mobile applications have distinct characteristics that may differentiate privacy considerations from other mobile applications in other domains. While the use of smartphone sensors such as GPS, accelerometer, or gyroscope may be similar to other mobile apps, the analysis and processing of data captured during vehicle movements may serve a different, more sensitive purpose: information about driving style, such as speed and safety, as well as information about daily routines can be derived (Cichy et al., 2021), too. Extant research (e.g., Derikx et al. 2016; Streich et al., 2018; Walter and Abendroth, 2020) shows that privacy considerations are relevant for using and designing connected car services. Users may associate a variety of negative consequences with the sharing of car data, such as fees and fines for driving misbehavior, the extraction of daily routines such as their driving routes (e.g., from home to work), and the use of shared vehicle data to determine their liability in accidents (Cichy et al., 2021). Our research will focus on how these concerns can be addressed through the use of privacy assurances taking into account context-specific risks (Xu et al., 2012) for the context of sharing driving-related data (Cichy et al., 2021).

In general, privacy assurances refer to "organizational measures that provide users with assurances about privacy protection" (Schulmeyer and Hess, 2022, p. 1). In this paper, we consider privacy assurances that are implemented as text-based privacy statements that may reduce users' privacy concerns and ultimately increase data disclosure (Hui et al., 2007; Xu et al., 2008). Here, our study focuses on the effect of short privacy assurance statements, and we do not consider mandatory and comprehensive privacy policies. In general, similar to Mousavi et al. (2020), we generally consider the threat appraisal process of protection motivation theory (PMT) (Rogers, 1975; Vance et al., 2012) our theoretical lens. In addition to the relatively well-understood, more general privacy assurances (e.g., Hudson and Liu, 2023; Keith et al., 2010; Mousavi et al., 2020), we aim to investigate how assurances targeting specific privacy risks impact privacy perceptions for driving-related data. Specifically, we intend to understand better whether a threat-specific privacy assurance is more effective than a general assurance in the context of connected vehicle applications and pose the following research question.

RQ: How do short, text-based privacy assurances of varying specificity published by app providers impact user perceptions in the context of privacy threats associated with sharing driving data?

Here, our research focuses on two data-intensive connected vehicles use cases: usage-based insurance (UBI) and traffic hazard warning apps. Vehicle drivers can use UBI to receive adjusted rates for their vehicle insurance based on their distinct driving behavior (Husnjak et al., 2015). We find this use case particularly interesting, since it is already relatively widely deployed, provides tangible benefits, and uses a broad range of privacy-sensitive data items such as speed, location, acceleration, and braking states (Arumugam and Bhargavi, 2019). As our second use case, we consider apps that can provide traffic hazard warnings to improve traffic safety (Trager et al., 2021), but more specifically those where user data is used to derive more concrete and timely information. We consider this use case to be relevant since it is generally comparable to UBI in the domain of traffic safety and, depending on the implementation, in terms of data captured, but it differs in terms of the incentive to use it.

The practical motivation for our research stems from examining privacy assurance statements in real-world examples found in the Google Play Store. For example, for usage-based insurance, such statements can, in addition to the mandatory privacy policies, be found in the app store descriptions of the German apps "Allianz BonusDrive" (Allianz Deutschland, 2023), "LVM-Go4Smile" (dibera GmbH, 2023), and "Kfz Vario FahrStil SAARLAND" (Saarland Versicherungen, 2021). While all three

descriptions assure that data will be processed in accordance with applicable privacy regulations, the former two additionally state that data is in safe hands (translated). The "Allianz BonusDrive" app store description text also explicitly states that data will not be shared with other parties, such as the police (translated). Even more extensive explanations regarding privacy-friendly data handling can be found on the websites of the insurance companies (Allianz, 2023; LVM Versicherung, 2023; SAARLAND Versicherungen, 2023).

Thus, our study intends to contribute to privacy research in the context of connected vehicles and offer furtherninsights into how users perceive information privacy for driving-related apps. For example, the benefit of employing privacy-friendly measures can be better understood by understanding the impact of privacy assurances. Furthermore, we aim to advance research on privacy assurances for connected objects by considering their specificity. We conducted an explorative, between-subjects online experiment based on fictional app store pages with two different experimental setups. Text-based online experiments are commonly used to investigate user perceptions towards mobile applications, often focusing on download intentions as a first step towards app usage (e.g., Gu et al., 2017; Harborth and Pape, 2021).

2 Privacy in the Context of Connected Vehicles

2.1 Connected vehicle applications

The term connected vehicle typically refers to digital systems in a vehicle that connects it to its environment, such as other vehicles or infrastructure, and includes a wide range of use cases such as infotainment, telematics, traffic safety, and advanced driver assistance systems (Lu et al., 2014; Uhlemann, 2015). Following this definition, we also consider connected, driving-related smartphone applications as part of the connected vehicle experience. For example, these applications may be connected to the vehicle manufacturer's back-end systems to directly access vehicle data collected by vehicle sensors, which is then transmitted to the manufacturer via the connected vehicles' telematics units, or they may be standalone mobile applications where smartphone sensors collect vehicle movement data (Kaiser et al., 2021; Reich et al., 2018). Connected vehicle services can be grouped into six broad categories: safety and security, convenience, cost-reduction, traffic efficiency, infotainment, and data accessibility (Sterk et al., 2022).

For example, apps that provide information about road hazards and dangerous driving, as described by Trager et al. (2021), typically warn drivers of dangerous spots, situations, or behaviors. A concrete instantiation of such a system could be an application providing information about accident hotspots based on historical data as developed by Ryder et al. (2021). Other systems may utilize smartphone sensors such as GPS and IMU to detect hazards like potholes (e.g., Mednis et al., 2011) and share this information with others. Further applications may attempt to detect the driving style and, if necessary, encourage the individual driver to drive more carefully (e.g., Kaiser et al., 2020).

With regard to safe driving, a relevant use case is insurance telematics that enable UBI (Händel et al., 2014; Soleymanian et al., 2019; Vavouranakis et al., 2017) to varying degrees: While some types of UBI simply operate as a pay-as-you-drive (PAYD) model, i.e., consider how frequently customers use their vehicle, others, known as pay-how-you-drive (PHYD), evaluate driving behavior and leverage various metrics to determine a safety rating, e.g., in the form of a driving score (Tselentis et al. 2017). For example, metrics may comprise mileage, hard braking, cornering, speed, and smartphone use, and based on the achieved risk score, the customer is given a discount (Guillen et al., 2021; Soleymanian et al., 2019). Insurance telematics apps may vary in the hardware they require (Händel et al., 2014).

2.2 Privacy and User Acceptance

Collecting vast amounts of vehicle data to offer value-added services raises many ethical and privacy concerns; for instance, very detailed habits and mobility patterns can be derived from vehicle movement

data (Derikx et al., 2016; Koester et al., 2021). A public survey commissioned by FIA Region I (2016) in 12 European countries on consumer awareness of connected vehicles shows a discrepancy between what European citizens are willing to accept and the data that car manufacturers collect and concludes that citizens want to decide with which services providers their data is shared. Data about connected cars can be sensitive, and the services offered could harm the car user, e.g., leading to higher insurance charges in case of harsh driving (Pumplun et al., 2021). Recently, Cichy et al. (2021) explored users' privacy-related concerns and the impact of psychological ownership. They found that users associate various different negative consequences with sharing vehicle data, for example, ranging from the threat of fines and prosecution to the less prevalent fear of vehicle data being used to help position radar traps more effectively. Overall, many empirical studies investigate privacy concerns for connected car applications and consider them in relation to the application context, such as the type of organization collecting the data, the type of data itself, and the use case (e.g., Endo et al., 2016; Derikx et al., 2016; Walter and Abendroth, 2020). In this regard, researchers often analyze the relationship between privacy concerns and the intention to disclose information or use a service (e.g., Buck and Reith, 2020; Koester et al., 2021). Other research provides insights whether drivers are sufficiently informed about the use of data in connected vehicles (Bella et al., 2021).

Usage-based insurance collects a plethora of data about drivers and their driving behavior to calculate premiums, which raises privacy concerns (Derikx et al., 2016). As a result, several studies have investigated the acceptance of such insurance models with different results. For example, Sahebi and Nassiri (2017) found that drivers of cheaper vehicles, middle-aged drivers, and risk-averse drivers were more likely to accept a UBI scheme that includes a connected vehicle system that provides warnings for traffic hazards. In another study, Śliwiński and Kuryłowicz (2021) concluded that only few study participants would refuse to have their driving style monitored if they receive a discount on their insurance. However, UBI system users reported knowing that behavioral patterns can be derived from GPS location, which can be used for more than just calculating premiums (Quintero and Benenson, 2019). Derikx et al. (2016) used conjoint analysis and found that while consumers prefered their current insurance products to usage-based car insurance, privacy concerns could be reduced, if offered a small financial compensation.

3 Theoretical Background and Research Design

3.1 Theoretical lens

Information privacy concerns an individual's control over their data and is a long-standing research topic gaining importance with the ubiquity of online services such as social media, online shopping, and location-based services (Bélanger and Crossler, 2011; Smith et al., 2011). In IS research, several theories and models explain how privacy concerns impact user behavior and how the intention to disclose information is formed (Bélanger and Crossler, 2011; Li, 2012). According to privacy calculus theory, users base their decision to disclose information on a trade-off between the benefits of disclosure and possible risks (Culnan and Armstrong ,1999; Laufer and Wolfe, 1977; Li, 2012). Privacy calculus theory is commonly used to understand information disclosure intentions in the context of mobile apps, for example, by Keith et al. (2013) or Wang et al. (2016). On the other hand, protection motivation theory (PMT) concerns the threat/risk vulnerability and severity in combination with an individual's ability to cope with threats (Rogers, 1975; Vance et al., 2012). PMT is a common theory for explaining privacy-related behavior in IS research (Li, 2012) and is highly relevant for privacy assurances (e.g., Mousavi et al., 2020): Essentially, users conduct a threat appraisal based on the perceived susceptibility and severity of privacy risks, and simultaneously, a coping appraisal is conducted, e.g., regarding self-efficacy and response efficacy (Rogers, 1975; Vance et al., 2012). This theory is often used in the context of information security (e.g., Tsai et al., 2016). We would like to note that in this paper, we use the terms risk and threat interchangeably and call the risk susceptibility and vulnerability the risk probability.

Apart from PMT, specifically in the context of privacy assurances, e.g., in Bansal et al. (2015), Gu et al. (2017), or Lowry et al. (2012), a commonly employed theory is the Elaboration Likelihood Model (ELM). The ELM deals with an individual's ability and motivation to process a message based on argument quality and peripheral cues (Petty and Cacioppo, 1986; Kitchen et al., 2014).

3.2 Privacy assurances

Regarding the user perspective, one research stream deals with privacy nudging, i.e., influencing user privacy decisions (Ioannou et al., 2021). For example, Almuhimedi et al. (2015) show that most users reassess their app permissions when provided with information about the amount and type of third parties with which their data is shared. A relevant tool to influence users' privacy perceptions is privacy assurances in the form of textual statements and seals (Hui et al., 2007; Xu et al., 2008), and many studies are addressing these or similar phenomena. In the context of a study on a fictional restaurant review app, Gu et al. (2017) used the ELM and found that permission sensitivity and justification as central factors and app popularity as a peripheral cue significantly affect privacy concerns. Similar to our research, Keith et al. (2010) analyzed the impact of privacy assurances on app store pages in the context of location-based services. They found them to be a significant factor in reducing privacy concerns, and one of the app scenarios used in their experiment was a mobile app providing live feedback on traffic. Similarly, in a study conducted by Wang and Herrando (2019) in the context of social commerce, institutional privacy assurances positively affected trust, thereby increasing purchase intentions. Mousavizadeh and Kim (2015) found that privacy assurance statements reduce threat susceptibility. Hudson and Liu (2023) compared the effect of privacy assurance statements concerning the compliance with the specific privacy regulations between European and Chinese mobile users, and they found them not to be effective in reducing privacy concerns for European users. Related to privacy assurance statements, Betzing et al. (2020) conducted an online experiment on data use transparency for app permission requests and found no significant difference in the outcome when transparency features were present. In a study conducted by Zeng et al. (2022) in the context of e-commerce, the presence of a privacy policy as a privacy assurance led to decreased purchases, and the authors considered the customers' increased awareness of negative outcomes as a relevant factor. This aligns with other studies not directly related to privacy assurance. For instance, Mamonov and Benbunan-Finch (2018) found that the awareness of privacy threats increases privacy-protective behavior. In their study, participants were presented with news articles about threats, and information disclosure intention and password strength were measured afterward. Similarly, Spears (2013) found that the awareness of privacy threats leads to avoiding risky behavior.

Although our paper only provides a brief overview of some relevant literature, in sum, some research finds privacy-relevant communication effective in reducing privacy concerns, while others find negligible or even negative effects. We want to again note that the privacy assurance statements we consider are generally similar to privacy policies which can also be considered privacy assurances (Xu et al., 2008). However, the privacy assurance statements considered in our study are shorter and can therefore be placed more prominently, and they are meant to be provided in addition to mandatory and comprehensive privacy policies and statements.

3.3 Research design and hypotheses

We aim to contribute to privacy research in the context of connected car applications and to advance the understanding of what contextual factors, in this case, types of privacy assurance statements, affect privacy perceptions in different connected car use cases. We base our research design on related literature, with some deviations and simplifications. First, similar to Gu et al. (2017), we utilize download intention to measure initial usage intention because we believe that a text-based experiment with app store pages is insufficient to indicate long-term use reasonably. Second, similar to research such as Pumplun et al. (2021), we follow the privacy calculus theory, and, in this regard, we assume that download intention is related to information disclosure intention and therefore depends on the interplay

of privacy concerns and perceived usefulness. As two key constructs, we use, like Mousavi et al. (2020), risk probability and severity (also called threat susceptibility/vulnerability and severity) from the threat appraisal process in PMT, and in our research, we consider the assurance mechanism to affect threat perception in terms of these two constructs directly. Likewise, we assume they are relevant antecedents of privacy concerns, privacy protection and disclosure intentions (e.g., Mousavi et al., 2020; Rodriguez-Piero et al., 2022). In addition, trust is considered a relevant construct in privacy research that can act as an antecedent, moderator, or outcome of privacy (Smith et al., 2011).

Our research design assumes that situation-specific privacy concerns are negatively related to usage intentions, although the literature is not entirely conclusive in this regard (e.g., Buck and Reith, 2020; Rejikumar, 2013). If privacy were irrelevant for decisions to use connected car services, this would imply that assurances would likely not be beneficial for increasing app usage. However, we see sufficient evidence in the literature that privacy is indeed very relevant for connected car services (Cichy et al., 2021; Koester et al., 2022). Therefore, based on the described research background, we assume that privacy assurances increase usage intentions by reducing privacy concerns since assurance statements may reduce the perceived probability that privacy threats will occur (Mousavizadeh and Kim, 2015) when using the connected car service.

H1: Privacy assurance statements provided by app vendors of driving-related mobile applications alter privacy-related perceptions, resulting in reduced privacy concerns.

However, as discussed in the previous section, we also acknowledge that there may be a countervailing effect at play: Users may lack immediate awareness of the types of data collected and the specific threats in the context of connected cars (e.g., Bella et al., 2021). In this case, explicitly mentioning these aspects in privacy assurance statements may increase user awareness, potentially leading to detrimental effects on privacy concerns and increased privacy-protective behavior, i.e., not downloading the app (e.g., Mamonov and Benbunan-Finch, 2018; Zeng et al., 2022). Overall, we hypothesize that privacy assurances have an effect beyond the specific apps by increasing awareness of privacy threats. Building on the previous sections, we assume that if a threat-specific assurance is present, this threat will be perceived as more severe by users in general because users may subconsciously attribute higher importance to this threat. Similarly, we hypothesize that a threat-specific assurance will decrease the perceived general probability or likelihood of the threat occurring. We assume this may be the case because privacy assurances may lead users to believe that companies are taking steps to prevent this threat.

H2a: Threat-specific privacy assurance statements increase the perceived <u>severity</u> of the respective threat.

H2b: Threat-specific privacy assurance statements decrease the perceived <u>probability</u> of the respective threat.

Nevertheless, there could also be a direct benefit from more specific privacy assurance statements. For example, extant research shows that more vague privacy policies are associated with reduced data disclosure (Bhatia et al., 2016). In our view, this could point to a positive effect of more concrete privacy assurance statements.

4 Experiment Design and Data Collection

We used two experimental setups to investigate our research questions and test our hypotheses empirically. Study participants were presented with an app store mock-up related to UBI, as shown in Figure 1, and asked to assume that they have to decide whether they want to download the app. Participants should assume that the app is compatible with their vehicle and insurance company. The app store page was simplified and included information about the app's functionality and data use. By simplifying the page, we aim to reduce peripheral cues, such as app ratings or screenshots, which could potentially affect privacy concerns (e.g., Gu et al., 2017). The fictional app store page of the warning app is similar, referring to an app that collects data to identify traffic hazards, which are shared with

other app users who are then warned accordingly. Therefore, the 'data use' section of both use cases is almost identical.

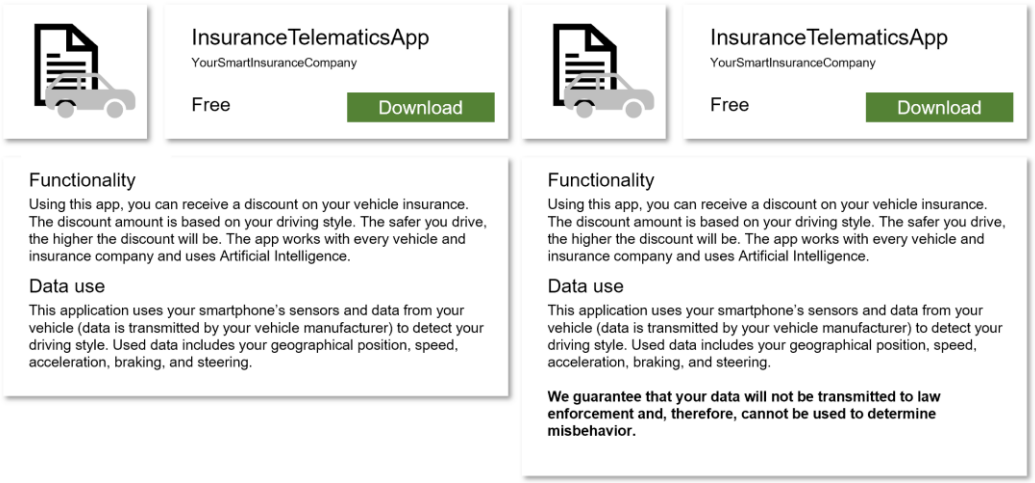

Figure 1. App store pages presented to group C_UBI and group S1_UBI (translated from German)

The first experimental compraison consists of *four participant groups* (see Table 1) to compare two different use cases in the context of the *presence of a general privacy assurance statement*. The assurances used are based on the research conducted by Cichy et al. (2021) and our observations of real-world UBI apps. The treatment groups (T) received a general privacy assurance (translated): *"Data collected by this app is in safe hands with us and will be processed in accordance with the General Data Protection Regulation."*

	Usage-based insurance	Traffic hazard warning
No privacy assurance	C_UBI	C_WA
General privacy assurance	T_UBI	T_WA

Table 1. First experimental setup covering both use cases

In the second experiment (see Table 2), we use the UBI application case to investigate the impact of *two threat-specific privacy assurances*; the threats were selected and adapted from Cichy et al. (2021, p. 1870). Here, an additional treatment group (S1_UBI) received a privacy assurance relating to a prevalently stated (Cichy et al., 2021), specific negative consequence in the context of connected car data sharing (translated*): "We guarantee that your data will not be transmitted to law enforcement and, therefore, cannot be used to determine misbehavior."* The second additional group's (S2_UBI) app page stated an assurance regarding a less prevalenty stated (Cichy et al., 2021) negative consequence (translated): *"We guarantee that your data will not be used for advertising (e.g., by car dealers or repair shops)."*

No privacy assurance	General privacy assurance	Threat-specific assurance	Threat-specific assurance
C_UBI	T_UBI	S1_UBI	S2_UBI

Table 2. Second experimental setup in the context of usage-based insurance.

Our study was primarily conducted in German, so all survey quotes are translated into English. Privacy assurance statements were printed in bold font. However, we did not include any comprehension checks on the same survey page and did not explicitly state that participants should read the app store page carefully. This was deliberately done because we assumed that in a real-world scenario, users may not always fully comprehend an app store page in its entirety before downloading the app, and we also did not want to increase possible demand effects in the survey. Therefore, at the end of the survey, we only

asked participants whether the respective assurance statement was present on the app store page to determine whether participants were aware of the experimental manipulation.

Furthermore, participants were also asked to rate the app on multiple survey items relating to the constructs of our research design. We selected and adapted the items from the literature and measured them on a 7-point Likert scale, ranging from "Strongly disagree" (1) to "Strongly agree (7)". Following our research concept, the questionnaire included items on download intention (adapted from Gu et al., 2017) and trust (adapted from Cichy et al., 2021 based on Tax et al., 1998). In addition, we adapted and selected items from Mousavi et al. (2020) on privacy concerns, privacy risk probability (threat susceptibility), and privacy risk severity (threat severity). Mousavi et al. (2020) based the former constructs partly on Kim et al. (2008) and the latter two on Johnston and Warkentin (2010). In terms of adapting the items for privacy risk probability and severity to our context, we also considered the items used by Keith et al. (2013). We measured usefulness by including two items related to this construct (adapted from Cheng et al., 2006 based on Davis, 1989). Next, and on a new survey page, participants were asked to enter the negative consequences associate with sharing vehicle data for using digital services. They had to rate the likelihood and severity of different potential consequences (selected and adapted from Cichy et al., 2021, p. 1870) they perceive when sharing car data using digital systems. Thereby, we intended to determine whether privacy assurances alter threat perceptions beyond the specific app scenario.

For the experiment, we collected data by recruiting paid survey participants (n=297, mean age=31.59) through the survey platform *Prolific*, which has been shown to have high response quality (Peer et al., 2017). We used the platform's prescreening features to select participants with German as first language and who use a car at least once a month. The participants for the use case of the warning system were recruited in a separate batch from the UBI use case. Using crowd-worker platforms to gather survey participants is a common approach in IS research, and we followed best practices whenever possible (Jia et al., 2017). We extended our dataset with a smaller sample of students and discarded all students who failed the attention checks and did not have a driving license resulting in 132 additional participants (mean age=24.14). We also conducted a confirmatory factor analysis resulting in discarding a single item from the trust construct with a factor loading below 0.5 (e.g., Bagozzi and Yi, 1988). We found that we had not adapted this item correctly to our use case, resulting in ambiguous wording. For the data analysis described in the following section, we used the software IBM SPSS Statistics (IBM Corp., 2021) for all significance tests, and the Python package Seaborn (Waskom, 2021) was partially used to generate the boxplots.

5 Results

5.1 General privacy assurances

For the first experimental comparison, 278 participants with a mean age of 28.6 years were included in the final dataset after removing participants who did not complete the survey or failed the attention and prescreening checks. We did not exclude participants who were unaware of the assurance (reflecting potential real-world behavior of inattentive reading). The mean construct scores for all four groups are shown in Table 3, and for some constructs, the differences between the groups are visualized as boxplots in Figure 2. First, the presence of a general privacy assurance did not alter privacy concerns and perceived risk severity much, but the perceived risk probability was lower on average. Download intention was actually lower for group $T_{\_WA}$ compared to $C_{\_WA}$. We ran t-tests between each control and treatment group and found no significant difference between groups, except for the perceived risk probability between groups $C_{\_WA}$ and $T_{\_WA}$ (two-tailed p=0.023). However, we do not consider this an entirely reliable result in exploratory data analysis. Therefore, apart from a slight observed tendency of perceived lower privacy risk probability, the general privacy assurance did not seem to yield any benefit. Most importantly, the experimental comparison showed no clear benefit regarding privacy concerns and download intention. Second, there seem to be only small differences when considering the two different

use cases. Overall, for the warning app, download intention and perceived usefulness are rated slightly higher, and privacy concerns, risk probability, and risk severity are slightly lower. We ran t-tests between C_{UBI} and C_{WA} as well as T_{UBI} and T_{WA} and found significant differences for the constructs risk severity (two-tailed p=0.016) and download intention (two-tailed p=0.028) for the former and risk severity (two-tailed p=0.046) for the latter. Again, due to the exploratory nature of the comparison with multiple uncorrected tests (see, for example, Armstrong (2014)) and only small differences between groups, the results need to be interpreted more carefully, and further research would be necessary to determine entirely conclusive results.

	Usage-based insurance		**Traffic hazard warning app**	
With privacy assurance?	No (C_{UBI})	Yes (T_{UBI})	No (C_{WA})	Yes (T_{WA})
# Participants (n=278)	78	75	61	64
Mean age (28.6)	29.67	28.92	27.08	28.36
Awareness of assurance[1]	n.a.	33/33/9	n.a.	33/24/7
Download intention	**3.99** (1.97)	**3.97** (1.9)	**4.7** (1.71)	**4.3** (1.55)
Usefulness	**4.74** (1.54)	**4.6** (1.62)	**4.95** (1.62)	**4.84** (1.42)
Trust	**4.11** (1.34)	**4.04** (1.29)	**4.05** (1.39)	**3.99** (1.14)
Privacy concerns	**5.08** (1.45)	**4.76** (1.47)	**4.64** (1.57)	**4.64** (1.48)
Risk probability	**4.49** (1.44)	**4.15** (1.52)	**4.39** (1.49)	**3.81** (1.34)
Risk severity	**4.71** (1.54)	**4.67** (1.36)	**4.1** (1.35)	**4.19** (1.44)

[1] # Yes / # Not sure/Maybe / # No

Table 3. Results of the first experimental comparison (mean and standard deviation).

Nevertheless, differences in perceived risk severity could exist, for example, due to different data-processing parties (insurance vs. app provider), although trust did not seem to differ much. Both use cases involve traffic safety, although only UBI offers a tangible monetary benefit. Therefore, while we would have expected some clearer differences in usefulness and download intention, similar construct scores seem reasonable. From a usefulness perspective, comparing the app use cases may depend on specific information regarding the monetary benefit of the UBI and the safety benefit of traffic hazard warnings, which were not included in our app store descriptions. Overall, we found some evidence supporting H1 regarding the perceived probability of privacy risks but no support for the privacy assurance statements affecting privacy concerns.

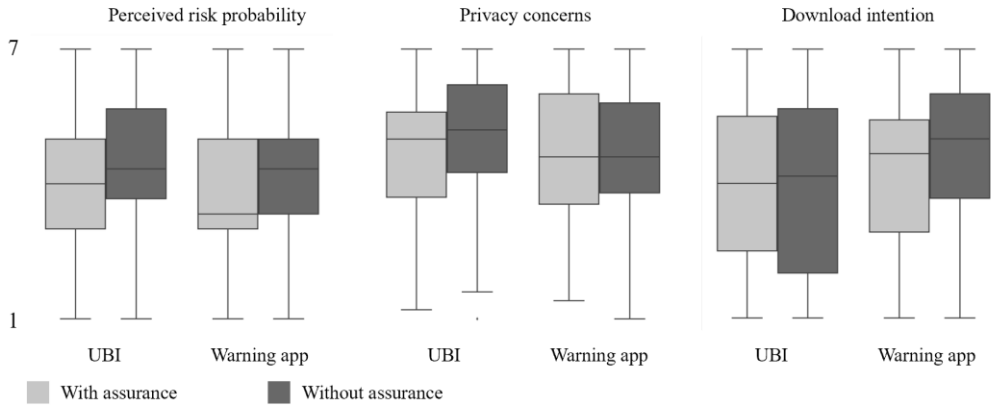

Figure 2. Visualized differences between groups (7=Strongly agree (i.e., very high), 1=Strongly disagree (i.e., very low)).

We also manually inspected the distribution of construct ratings and found that privacy concerns were slightly left skewed, i.e., most participants reported being concerned about their privacy. Also, download intentions were relatively prevalent at the extremes (i.e., strongly agree and strongly disagree), resulting in high standard deviations compared to the other groups meaning that participants appeared to be relatively decisive in their choice. Therefore, we also conducted Mann-Whitney-U tests (Mann and Whitney, 1947) which yielded no different insights. In our questionnaire, we asked participants if they usually read the app store page before downloading apps (measured on a scale of 1 to 7), as this indicates a requirement for being susceptible to app store privacy assurances in the first place. On average, all privacy-related constructs, i.e., risk severity, risk probability, and privacy concerns, are slightly higher for participants who usually read most of the app descriptions, although the correlations are relatively low. This may indicate that people concerned about their privacy tend to assess apps more carefully before downloading them, or vice versa.

5.2 Threat-specific privacy assurances

We consider the second main experimental comparison of threat-specific privacy assurances in the next step. Table 4 shows the mean construct ratings for each group. No significant differences between the groups were found using a one-way ANOVA, indicating that neither general nor threat-specific privacy assurances yield clear app-related benefits. In terms of awareness of the assurance statements, most participants correctly indicated that the respective textual statement was present. However, the "Maybe/Don't know" response type was prevalent in the T_{UBI} group with the broad, unspecific privacy assurance. This may indicate that participants can better notice or remember more specific statements.

	C_{UBI}	**T_{UBI}**	**$S1\_{UBI}$**	**$S2\_{UBI}$**
With privacy assurance?	No	General	Threat-specific	
# Participants	78	75	78	73
Mean age	29.67	28.92	29.72	31.53
Awareness of assurance[1]	n.a.	33/33/9	63/11/4	40/22/11
Download intention	**3.99** (1.97)	**3.97** (1.9)	**3.86** (1.97)	**3.84** (2.11)
Usefulness	**4.74** (1.54)	**4.6** (1.62)	**4.73** (1.68)	**4.46** (1.84)
Trust	**4.11** (1.34)	**4.04** (1.29)	**3.97** (1.34)	**3.79** (1.55)
Privacy concerns	**5.08** (1.45)	**4.76** (1.47)	**5.27** (1.31)	**5.16** (1.42)
Risk probability	**4.49** (1.44)	**4.15** (1.52)	**4.44** (1.53)	**4.22** (1.45)
Risk severity	**4.71** (1.54)	**4.67** (1.36)	**4.53** (1.59)	**4.59** (1.4)

[1] # Yes / # Not sure/Maybe / # No

Table 4. Results of the second experimental comparison (mean and standard deviation).

As explained above, at the end of our questionnaire, we asked participants about the probability and severity of general (i.e., not directly related to the app's use case) potential consequences of sharing car data. We assumed that threat-specific privacy assurances would alter the perception of a privacy threat in a specific domain beyond the concrete app scenario. We found that the app store's threat-specific assurances (S1 and S2) seem to reduce the perceived general probability of the threat mentioned in the privacy assurance occurring, as shown in Table 5. For example, participants exposed to the assurance that data will not be transmitted to law enforcement tend to see a lower probability of this threat when using connected car services than the other groups. To get an initial statistical overview, we tested for significance using a one-way ANOVA followed by the pair-wise least significant difference (LSD) tests (the LSD tests are relatively lenient, i.e., results are more likely to be significant (e.g., Williams and Abdi (2010)). Both data transmission to the police and data use for advertising showed significant

differences between groups at a 95% confidence level (p=0.024 and p= 0.015, respectively). The LSD-tests showed significant differences for S1 compared to all other groups for data transmission to the police (C: p = 0.01, T: p = 0.014, S2: p = 0.013) and for data use for advertising between group S2 compared to C (p = 0.002) and T (p = 0.017). No significant differences were found between the groups at a 95% confidence level for the other privacy threats.

Consequence/threat	**C_UBI**	**T_UBI**	**S1_UBI**	**S2_UBI**
Data used to determine liability in case of an accident.	5.29 / 3.94	5.48 / 4.08	5.21 / 4.09	5.63 / 4.38
Data transmitted to police/authorities which can be used to determine misbehavior.	5.01 / 5.14	4.98 / 5.25	4.27 / 5.29	5 / 5.3
Extraction of information about daily routines that could be useful for advertisements/burglars.	6.17 / 6.17	5.99 / 6.09	5.63 / 6.01	6 / 6.15
Increased vehicle insurance costs or car rental costs.	5.88 / 5.71	5.81 / 5.45	5.54 / 5.74	5.84 / 5.81
Advertisements (e.g., by car dealers or repair shops).	5.83 / 4.9	5.68 / 4.89	5.44 / 4.69	5.08 / 4.99

Table 5. Comparison of the mean perceived probability/severity of potential consequences (translated and shortened) when sharing car data selected and adapted from Cichy et al. (2021, p. 1870) (1=very unlikely, 7=very likely / 1=Not severe/bad, 7=Very severe/bad).

We would like to note that most variables were not normally distributed. Although we assume that the statistical tests used are usually sufficiently robust (e.g., Norman, 2010), we confirmed the ANOVA results with a non-parametric test, and in this case, the Kruskal-Wallis test (Kruskal and Wallis, 1952) was used. The Kruskal-Wallis test still indicated significant differences between groups at a 95% confidence level for data transmission to the police and data use for advertisements. However, in the pair-wise posthoc comparisons (with Bonferroni adjustment, see, e.g., Armstrong, 2014), for data transmission to the police, group S1 was only significantly different from other groups at a 90% confidence level. Group S2 was only significantly different for data use for advertisements compared to group C (p = 0.02). While these results at least partially support hypothesis H2b concerning risk probability, indicating that threat-specific privacy assurances may reduce the perceived probability of the specific threat occurring in general, the results were not entirely clear and reliable from a statistical point of view. Moreover, group S1 had the lowest probability for all threats except for advertisements. For this reason, we again believe that further research is needed to ensure that this effect holds across other samples, threats, and application cases. For the severity of threats, no significant differences were found between the groups, and therefore, we do not find any support for hypothesis H2a.

6 Discussion, Implications, and Limitations

6.1 Result overview

Overall, in contrast to other literature, we found no clear evidence that the presence of a general privacy assurance statement significantly impacts any app-related privacy perceptions and download intentions. However, as discussed in Section 2.2 and 2.3, this was not entirely unexpected. In our opinion, several factors may contribute to this finding. First, the positive effect of the assurance may be offset by a negative effect due to increased threat awareness. As mentioned, research shows that making users aware of threats increases privacy-protective behavior (e.g., Manomov and Benbunan-Fich, 2018). Second, it could be argued that participants did not sufficiently read or understand the privacy assurance statements. As explained, we asked whether participants generally read the app store page before downloading an app (1=Not at all, 7=Yes, fully) which yielded a mean of 4.32, with a higher level for group S1 (mean=4.95). This could explain why the percentage of participants confirming the presence

of the privacy assurance statement was highest for S1. Third, as mentioned in extant research (Walter and Abendroth, 2018), insurers and app providers were rated as two of the least trusted parties regarding car data privacy, and participants may simply not believe the assurance statement to be reliable. Our study must also be viewed in light of the privacy paradox, where an individual's stated behavior regarding privacy differs from their actual behavior (Kokolakis, 2017; Norberg et al., 2007). We see this as an inherent limitation of the text-based scenario as opposed to field studies. In terms of threat-specific privacy assurances, we found no clear benefits for app-related perceptions of privacy. Nevertheless, the privacy assurances appear to reduce the perceived probability of the threat mentioned in the assurance occurring in general, although this result is also not entirely conclusive. If this observation holds for other threat types, sample populations, and application cases, then threat-specific assurances may be advantageous to some degree in fostering the general adoption of connected and autonomous cars by reducing the perceived probability of privacy risks related to driving data sharing.

We explicitly want to emphasize that our research is exploratory. First, our sample size is relatively small. Second, our study results may be strongly influenced by the design of the presented app store page, e.g., the screen position, font size, font color of the privacy assurances, and their wording. Additionally, usage-based insurance and warnings apps are only two use cases within the broad field of connected vehicle applications. We think that the results may strongly depend on the use case, because driving-related applications differ in the benefits they provide to the user (e.g., safe driving, financial benefits, driving comfort) and in the data they require (e.g., location-related information, driving style, and behavior data). Studies such as Walter and Abendroth (2018) show that privacy perceptions differ regarding the collected data types and data processing parties. Furthermore, user attitudes may be influenced by prior experience with insurance companies and by prior experience with related apps. Finally, as in similar studies (e.g., Cichy et al., 2021), the participants' background may lead to unnoticed biases, e.g., because all participants are from Germany. As found by Hudson and Liu (2023) privacy assurances can lead to different effects based on the country where they are employed. In Germany, as part of the European Union, information privacy is regulated by the relatively strict General Data Protection Regulation (GDPR) (Hoofnagle et al., 2019), so additional privacy assurance could be perceived superfluous. However, there may also be an increased awareness or consciousness of information privacy (e.g., Kulyk et al., 2020). For example, there may be country and city-specific differences in technological availability and infrastructure for connected and autonomous vehicles (Khan et al., 2019; KPMG International, 2020).

We also revisited our open-ended question in the survey, where participants were asked to indicate perceived negative consequences associated with sharing vehicle data. Here, our results were very similar to the work by Cichy et al. (2021). Concerns about increased costs (e.g., vehicle insurance) and general tracking (via location data) were common across all groups. Data transmission to police/authorities, data used for advertisements, and errors when processing data were also stated relatively frequently. Apart from specific negative consequences, many participants had general privacy-related concerns, such as the data-requesting party not adhering to privacy regulations, abuse of data, or violation of privacy. Only very few participants stated that they are not concerned.

6.2 Implications and future research

With our research, we advance the understanding of the role of privacy assurances in the context of connected vehicles and further investigate the interplay between privacy assurances and privacy concerns, especially regarding threat appraisal. In light of our findings, it appears questionable whether explicit privacy assurances on app store pages are an effective method to reduce privacy concerns in connected vehicles. Additionally, targeting these assurances to specific threats did not yield a clear benefit in our experiment. While the privacy assurances targeted at specific threats did appear to reduce the general perceived probability of that threat occurring, they did not appear to alter privacy perceptions of the app. One explanation could be that the threats in the context of connected cars are so diverse that changing the perception of a single threat does not reduce overall privacy concerns. Our experiments also did not show that assurances have a negative effect on privacy perceptions, so we cannot derive a

recommendation against privacy assurance statements, however, in our experiment download intentions were lower for group T_{WA} compared to C_{WA}.

Nevertheless, our study showed that privacy concerns and threats are generally relevant in the context of connected driving, given the relatively high mean scores for the privacy constructs. However, this poses the question of how privacy concerns in vehicle data sharing can be mitigated. In the context of connected cars, trust in parties receiving the data differs (Walter and Abendroth, 2018). Concerning smart and sustainable mobility systems, regulators are important in guiding aspects such as privacy and ethical issues (Ketter et al., 2022). This motivates thinking about the implications of data trustees and intermediaries to control access to vehicle data (e.g., Pretzsch et al., 2021). We find similarities to Sokoll (2021, Article 3), who showed that data certification in the context of connected cars could benefit at least some privacy perceptions. In addition, it may be that privacy assurances are only effective for specific subgroups of users. In our view, this is a reasonable assumption because many external factors were not included in our analysis. Most importantly, we did not fully account for factors relating to ELM, as for example, in Gu et al. (2017) and Lowry et al. (2012), and we cannot fully track how our participants processed the related information considering elaboration likelihood. If privacy assurances are especially effective for specific subgroups, it may make sense to design personalized privacy assurances that appeal to specific fears in the context of connected vehicle data sharing. As mentioned, our privacy assurances were short statements located on a fictional app store page, and we believe this is not a particularly invasive approach in practice. Another approach could be to display privacy assurances in the app. However, this would assume that the user has already downloaded the app, so the initial decision to use the app has already been made. It would therefore make more sense for permission requests (e.g., Gu et al., 2017) or in other situations where users have to decide whether they share their data (e.g., opt-in settings, agreement to privacy policy) (e.g., Walter et al., 2018).

Lastly, a contemporary research direction in information privacy is the role of (technical) privacy assurance techniques such as differential privacy (Xu and Dinev, 2022). The privacy assurance statements in our study were ultimately promises that did not include a justification of why these promises could be kept. In this regard, it would be interesting to analyze whether privacy assurances backed up by (sophisticated) privacy-friendly measures (technical or organizational) are more efficient. For example, app providers could explicitly state that data anonymization measures or techniques such as differential privacy (Hassan et al., 2020) are employed.

7 Conclusion

Our research investigated privacy assurances in the context of two smartphone-based connected vehicle applications, UBI, and traffic hazard warning. In doing so, we considered the impact of the type of privacy assurance on the privacy risk it should alleviate. For this purpose, we conducted a between-subjects online experiment with four groups for the case of usage-based insurance and two groups for traffic hazard warnings. While we found that threat-specific assurances appeared to alter general perceived threat probabilities, our results were primarily inconclusive, and we could not show that privacy assurances of any specificity significantly increased app-specific download intentions.

Acknowledgment

This work was supported by the Federal Ministry for Economic Affairs and Climate Action on the basis of a decision by the German Bundestag through project D-TRAS. This work has further received funding by the Austrian Research Promotion Agency (FFG) in the ICT of the Future program under project number 880046 (project D-TRAS). ICT of the Future is a research, technology, and innovation funding program of the Republic of Austria, Federal Ministry for Climate Action, Environment, Energy, Mobility, Innovation and Technology (BMK). The Austrian Research Promotion Agency (FFG) has been authorized for program management.

References

Aghayari, H., Kalankesh, L. R., Sadeghi-Bazargani, H., and Feizi-Derakhshi, M.-R. (2021). "Mobile applications for road traffic health and safety in the mirror of the Haddon's matrix," *BMC Medical Informatics and Decision Making* 21, 230.

Allianz (2023). "Telematik-Tarif: Allianz BonusDrive," URL: https://www.allianz.de/auto/kfz-versicherung/telematik-versicherung/ (visited on March 31, 2023).

Allianz Deutschland (2023). "Allianz BonusDrive," URL: https://play.google.com/store/apps/details?id=de.allianz.bonusdriveapp (visited on March 31, 2023).

Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J., Cranor, L. F., and Agarwal, Y. (2015). "Your Location has been Shared 5,398 Times!," in: B. Begole, J. Kim, K. Inkpen and W. Woo (eds.) *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, Seoul, Republic of Korea, 787-796.

Amarasinghe, M., Kottegoda, S., Arachchi, A. L., Muramudalige, S., Dilum Bandara, H. M. N., and Azeez, A. (2015). "Cloud-based driver monitoring and vehicle diagnostic with OBD2 telematics," in: *2015 Fifteenth International Conference on Advances in ICT for Emerging Regions (ICTer)*, Colombo, Sri Lanka, 243-249.

Armstrong, R. A. (2014). "When to use the Bonferroni correction," *Ophthalmic and Physiological Optics* 34 (5), 502-508.

Arumugam, S., and Bhargavi, R. (2019). "A survey on driving behavior analysis in usage based insurance using big data," *Journal of Big Data* 6, 86.

Athanasopoulou, A., Bouwman, H., Nikayin, F., and Reuver, M. de (2016). "The disruptive impact of digitalization on the automotive ecosystem: a research agenda on business models, platforms and consumer issues," in *Proceedings of the 29th Bled eConference: Digital Economy*, Bled, Slovenia, 597-604.

Bansal, G., Zahedi, F., and Gefen, D. (2015). "The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern," *European Journal of Information Systems* 24 (6), 624-644.

Bagozzi, R. P., and Yi, Y. (1988). "On the evaluation of structural equation models," *Journal of the academy of marketing science* 16, 74-94.

Bélanger, F., and Crossler, R. E. (2011). "Privacy in the digital age: a review of information privacy research in information systems," *MIS Quarterly* 35 (4), 1017-1041.

Bella, G., Biondi, P., and Tudisco, G. (2021). "Car Drivers' Privacy Concerns and Trust Perceptions," in: Fischer-Hübner, S., Lambrinoudakis, C., Kotsis, G., Tjoa, A. M., and Khalil, I. (eds.) *Trust, Privacy and Security in Digital Business*, Cham: Springer International Publishing, 143-154.

Betzing, J. H., Tietz, M., vom Brocke, J., and Becker, J. (2020). "The impact of transparency on mobile privacy decision making," *Electronic Markets* 30 (3), 607-625.

Bhatia, J., Breaux, T. D., Reidenberg, J. R., and Norton, T. B. (2016). "A theory of vagueness and privacy risk perception," in: *2016 IEEE 24th International Requirements Engineering Conference (RE)*, Beijing, China , 26-35.

Bohnsack, R., Kurtz, H., and Hanelt, A. (2021). "Re-examining path dependence in the digital age: The evolution of connected car business models," *Research Policy* 50 (9), 104328.

Buck, C., and Reith, R. (2020). "Privacy on the road? Evaluating German consumers' intention to use connected cars," *International Journal of Automotive Technology and Management* 20 (3), 297-318.

Cheng, T. E., Lam, D. Y., and Yeung, A. C. (2006). "Adoption of internet banking: An empirical study in Hong Kong," *Decision Support Systems* 42 (3), 1558-1572.

Cichy, P., Salge, T. O., and Kohli, R. (2021). "PRIVACY CONCERNS AND DATA SHARING IN THE INTERNET OF THINGS: MIXED METHODS EVIDENCE FROM CONNECTED CARS," *MIS Quarterly* 45 (4), 1863-1892.

Coppola, R., and Morisio, M. (2016). "Connected car: technologies, issues, future trends," *ACM Computing Surveys (CSUR)* 49 (3), 1-36.

Culnan, M. J., and Armstrong, P. K. (1999). "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science* 10 (1), 104-115.

Davis, F. D. (1989). "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Quarterly* 13 (3), 319-340.

Derikx, S., Reuver, M. de, and Kroesen, M. (2016). "Can privacy concerns for insurance of connected cars be compensated?" *Electronic Markets* 26 (1), 73-81.

Dhall, R., and Solanki, V. (2017). "An IoT Based Predictive Connected Car Maintenance," *International Journal of Interactive Multimedia and Artificial Intelligence* 4 (3), 16-22.

dibera GmbH (2023). "LVM-Go4Smile," URL: https://play.google.com/store/apps/details?id=de.lvm.go4smile (visited on March 31, 2023).

Endo, T., Nawa, K., Kato, N., and Murakami, Y. (2016). "Study on privacy setting acceptance of drivers for data utilization on connected cars," in: *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, Auckland, New Zealand, 82-87.

Engelbrecht, J., Booysen, M. J., van Rooyen, G.-J., and Bruwer, F. J. (2015). "Survey of smartphone-based sensing in vehicles for intelligent transportation system applications," *IET Intelligent Transport Systems* 9 (10), 924-935.

Faisal, A., Kamruzzaman, M., Yigitcanlar, T., and Currie, G. (2019). "Understanding autonomous vehicles," *Journal of Transport and Land Use* 12 (1), 45-72.

FEDERATION INTERNATIONALE DE L'AUTOMOBILE REGION I - EUROPE, THE MIDDLE EAST AND AFRICA (FIA Region I) (2016). "WHAT EUROPEANS THINK ABOUT CONNECTED CARS," URL: https://www.fiaregion1.com/wp-content/uploads/2017/06/FIA-Survey-Brochure-2016-web.pdf, (visited on March 31, 2023).

Gu, J., Xu, Y., Xu, H., Zhang, C., and Ling, H. (2017). "Privacy concerns for mobile app download: An elaboration likelihood model perspective," *Decision Support Systems* 94, 19-28.

Guillen, M., Nielsen, J. P., and Pérez-Marín, A. M. (2021). "Near-miss telematics in motor insurance," *Journal of Risk and Insurance* 88 (3), 569-589.

Händel, P., Skog, I., Wahlström, J., Bonawiede, F., Welch, R., Ohlsson, J., and Ohlsson, M. (2014). "Insurance Telematics: Opportunities and Challenges with the Smartphone Solution," *IEEE Intelligent Transportation Systems Magazine* 6 (4), 57-70.

Harborth, D., and Pape, S. (2021). "Investigating privacy concerns related to mobile augmented reality apps-A vignette based online experiment," *Computers in Human Behavior* 122, 106833.

Hassan, M. U., Rehmani, M. H., and Chen, J. (2020). "Differential Privacy Techniques for Cyber Physical Systems: A Survey," *IEEE Communications Surveys & Tutorials* 22 (1), 746-789.

Hoofnagle, C. J., van der Sloot, B., and Borgesius, F. Z. (2019). "The European Union general data protection regulation: what it is and what it means," *Information & Communications Technology Law* 28 (1), 65-98.

Hui, K.-L., Teo, H. H., and Lee, S.-Y. T. (2007). "The value of privacy assurance: An exploratory field experiment," *MIS Quarterly* 31 (1), 19-33.

Hudson, S., and Liu, Y. (2023). Mobile app users' privacy concerns: different heuristics for privacy assurance statements in the EU and China. *Information Technology & People*, 36 (1), 245-262.

Husnjak, S., Peraković, D., Forenbacher, I., and Mumdziev, M. (2015). "Telematics System in Usage Based Motor Insurance," *Procedia Engineering* 100, 816-825.

IBM Corp. (Released 2021). *IBM SPSS Statistics for Windows, Version 28.0*, Armonk, NY: IBM Corp.

Ioannou, A., Tussyadiah, I., Miller, G., Li, S., and Weick, M. (2021). "Privacy nudges for disclosure of personal information: A systematic literature review and meta-analysis," *PloS one* 16 (8), e0256822.

Jia, R., Steelman, Z., and Reich, B. H. (2017). "Using Mechanical Turk Data in IS Research: Risks, Rewards, and Recommendations," *Communications of the Association for Information Systems* 41, 301-318.

Johnston, A. C., and Warkentin, M. (2010). "Fear appeals and information security behaviors: An empirical study," *MIS Quarterly* 34 (3), 549-566.

Joy, J., and Gerla, M. (2017). "Internet of Vehicles and Autonomous Connected Car - Privacy and Security Issues," in: *2017 26th International Conference on Computer Communication and Networks (ICCCN)*, Vancouver, BC, Canada, 1-9.

Kaiser, C., Stocker, A., Festl, A., Lechner, G., and Fellmann, M. (2018). "A research agenda for vehicle information systems," in: *Proceedings of European Conference on Information Systems (ECIS) 2018*, Portsmouth, UK, 33.

Kaiser, C., Stocker, A., Viscusi, G., Fellmann, M., and Richter, A. (2021). "Conceptualising value creation in data-driven services: The case of vehicle data," *International Journal of Information Management* 59, 102335.

Kaiser, C., Stocker, A., Festl, A., Petrovic, M., Papatheocharous, E., Wallberg, A., Ezquerro, G., Orbe, J., Szilagyi, T., and Fellmann, M. (2020). "A Vehicle Telematics Service for Driving Style Detection: Implementation and Privacy Challenges," in: *Proceedings of the 6th International Conference on Vehicle Technology and Intelligent Transport Systems*, Prague, Czech Republic, 29-36.

Keith, M. J., Babb Jr, J. S., Furner, C. P., and Abdullat, A. (2010). "Privacy assurance and network effects in the adoption of location-based services: An iPhone experiment," *ICIS 2010 Proceedings*, 237.

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., and Greer, C. (2013). "Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior," *International Journal of Human-Computer Studies* 71 (12), 1163-1173.

Ketter, W., Schroer, K., and Valogianni, K. (2022). "Smart Sustainable Mobility: A Framework and Call for Action," *Forthcoming at Information Systems Research*. Available at SSRN: https://ssrn.com/abstract=4160719 (visited on March 31, 2023).

Khan, J. A., Wang, L., Jacobs, E., Talebian, A., Mishra, S., Santo, C. A., Golias, M., and Astorne-Figari, C. (2019). "Smart Cities Connected and Autonomous Vehicles Readiness Index," in: *Proceedings of the 2nd ACM/EIGSCC Symposium on Smart Cities and Communities*, New York, NY, USA, 8.

Kim, D. J., Steinfield, C., and Lai, Y.-J. (2008). "Revisiting the role of web assurance seals in business-to-consumer electronic commerce," *Decision Support Systems* 44 (4), 1000-1015.

Kitchen, P. J., Kerr, G., Schultz, D. E., McColl, R., and Pals, H. (2014). "The elaboration likelihood model: review, critique and research agenda," *European Journal of Marketing* 48 (11/12), 2033-2050.

Koester, N., Cichy, P., Antons, D., and Salge, T.-O (2021). "Privacy Risk Perceptions in the Connected Car Context," in *Hawaii International Conference on System Sciences* (2021), Honolulu, HI, USA.

Koester, N., Cichy, P., Antons, D., and Salge, T. O. (2022). "Perceived privacy risk in the Internet of Things: determinants, consequences, and contingencies in the case of connected cars," *Electronic Markets* 32, 2333-2355.

Kokolakis, S. (2017). "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon," *Computers & Security* 64, 122-134.

KPMG International (2020). "2020 Autonomous Vehicles Readiness Index," URL: https://assets.kpmg/content/dam/kpmg/xx/pdf/2020/07/2020-autonomous-vehicles-readiness-index.pdf (visited on March 31, 2023).

Kruskal, W. H., and Wallis, W. A. (1952). Use of ranks in one-criterion variance analysis. *Journal of the American statistical Association* 47 (260), 583-621.

Kulyk, O., Reinheimer, B., Aldag, L., Mayer, P., Gerber, N., and Volkamer, M. (2020). "Security and Privacy Awareness in Smart Environments – A Cross-Country Investigation," in: Bernhard, M., Bracciali, A., Camp, L. J., Matsuo, S., Maurushat, A. Rønne, P. B., & Sala, M. (eds.), *Financial Cryptography and Data Security*, Cham: Springer, 84-101.

Laufer, R. S., and Wolfe, M. (1977). "Privacy as a concept and a social issue: A multidimensional developmental theory," *Journal of Social Issues* 33 (3), 22-42.

Liao, S., Wilson, C., Cheng, L., Hu, H., and Deng, H. (2020). "Measuring the Effectiveness of Privacy Policies for Voice Assistant Applications," in: *Annual Computer Security Applications Conference*, Austin, Texas, 856-869.

Li, Y. (2012). "Theories in online information privacy research: A critical review and an integrated framework," *Decision Support Systems* 54 (1), 471-481.

Lowry, P. B., Moody, G., Vance, A., Jensen, M., Jenkins, J., and Wells, T. (2012). "Using an elaboration likelihood approach to better understand the persuasiveness of website privacy assurance cues for

online consumers," *Journal of the American Society for Information Science and Technology* 63 (4), 755-776.

Lu, N., Cheng, N., Zhang, N., Shen, X., and Mark, J. W. (2014). "Connected Vehicles: Solutions and Challenges," *IEEE Internet of Things Journal* 1 (4), 289-299.

LVM Versicherung (2023). "Telematik - LVM-Go4Smile: sicher fahren, clever sparen," URL: https://www.lvm.de/privatkunden/produkte/versicherungen/kfz-versicherung/lvm-go4smile-tab3 (visited on March 31, 2023).

Mamonov, S., and Benbunan-Fich, R. (2018). "The impact of information security threat awareness on privacy-protective behaviors," *Computers in Human Behavior* 83, 32-44.

Mann, H. B., and Whitney, D. R. (1947). "On a test of whether one of two random variables is stochastically larger than the other," *The Annals of Mathematical Statistics* 18 (1), 50-60.

Mantouka, E., Barmpounakis, E., Vlahogianni, E., and Golias, J. (2021). "Smartphone sensing for understanding driving behavior: Current practice and challenges," *International Journal of Transportation Science and Technology* 10 (3), 266-282.

Martínez-Pérez, B., La Torre-Díez, I. de, and López-Coronado, M. (2015). "Privacy and security in mobile health apps: a review and recommendations," *Journal of medical systems* 39 (1), 181.

Mednis, A., Strazdins, G., Zviedris, R., Kanonirs, G., and Selavo, L. (2011). "Real time pothole detection using Android smartphones with accelerometers," in: *2011 International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS)*, Barcelona, Spain, 1-6.

Merenda, M., Mazzullo, V., Carotenuto, R., and Della Corte, F. G. (2021). "Tiny Machine Learning Techniques for Driving Behavior Scoring in a Connected Car Environment," in: *2021 6th International Conference on Smart and Sustainable Technologies (SpliTech)*, Bol and Split, Croatia, 1-6.

Moon, S., Min, M., Nam, J., Park, J., Lee, D., and Kim, D. (2017). "Drowsy Driving Warning System Based on GS1 Standards with Machine Learning," in: *2017 IEEE International Congress on Big Data (BigData Congress)*, Honolulu, HI, USA, 289-296.

Mousavi, R., Chen, R., Kim, D. J., and Chen, K. (2020). "Effectiveness of privacy assurance mechanisms in users' privacy protection on social networking sites from the perspective of protection motivation theory," *Decision Support Systems* 135, 113323.

Mousavizadeh, M., and Kim, D. (2015). A study of the effect of privacy assurance mechanisms on self-disclosure in social networking sites from the view of protection motivation theory. *ICIS 2015 Proceedings*.

NORBERG, P. A., HORNE, D. R., and HORNE, D. A. (2007). "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors," *Journal of Consumer Affairs* 41 (1), 100-126.

Norman, G. (2010). "Likert scales, levels of measurement and the "laws" of statistics," *Advances in health sciences education : theory and practice* 15 (5), 625-632.

Peer, E., Brandimarte, L., Samat, S., and Acquisti, A. (2017). "Beyond the Turk: Alternative platforms for crowdsourcing behavioral research," *Journal of Experimental Social Psychology* 70, 153-163.

Petty, R. E., and Cacioppo, J. T. (1986). "The Elaboration Likelihood Model of Persuasion*," Advances in Experimental Social Psychology* 19, Leonard Berkowitz (ed.), Academic Press, 123-205.

Pretzsch, S., Drees, H., Rittershaus, L., Langdon, C. S., and Lange, C., Weiers, C. (2021). "MOBILITY DATA SPACE: SECURE DATA SPACE FOR THE SOVEREIGN AND CROSS-PLATFORM UTILIZATION OF MOBILITY DATA," URL: https://www.ivi.fraunhofer.de/content/dam/ivi/en/documents/brochure/Mobility_Data_Space_2021_EN_web.pdf, (visited on March 31, 2023).

Pumplun, L., Wiefel, J., Wächter, K., Barth, N., and Buxmann, P. (2021). "Smart Car Service Adoption: Investigating the Role of Information Privacy," in: *PACIS 2021 Proceedings*, Dubai, UAE, 60.

Quintero, J., and Benenson, Z. (2019). "Understanding Usability and User Acceptance of Usage-Based Insurance from Users' View," in *Proceedings of the 2019 2nd International Conference on Machine Learning and Machine Intelligence*, Jakarta, Indonesia, 52-57.

Reddy, T., and Premamayudu, B. (2019). "Vehicle Insurance Model Using Telematics System with Improved Machine Learning Techniques: A Survey," *Ingénierie des Systèmes d'Information* 24 (5), 507-512.

Reich, A., Krämer, N. A., and Lenninger, R. (2018). "Vehicle data mangement a standardized access as the basis of new business models," *ATZelektronik worldwide* 13 (2), 38-43.

Rejikumar, G. (2013). "A pre-launch exploration of customer acceptance of usage based vehicle insurance policy," *IIMB Management Review* 25 (1), 19-27.

Rodríguez-Priego, N., Porcu, L., and Kitchen, P. J. (2022). "Sharing but caring: Location based mobile applications (LBMA) and privacy protection motivation," *Journal of Business Research* 140, 546-555.

Rogers, R. W. (1975). "A protection motivation theory of fear appeals and attitude change1," *The journal of psychology* 91 (1), 93-114.

Ryder, B., Gahr, B., Egolf, P., Dahlinger, A., and Wortmann, F. (2017). "Preventing traffic accidents with in-vehicle decision support systems - The impact of accident hotspot warnings on driver behaviour," *Decision Support Systems* 99, 64-74.

Saarland Versicherungen (2021). "Kfz Vario FahrStil SAARLAND," URL: https://play.google.com/store/apps/details?id=de.sv.fahrstil (visited on March 31, 2023).

SAARLAND Versicherungen (2023). „Kfz Vario FahrStil," URL: https://www.saarland-versicherungen.de/content/versicherungen/kfz-versicherung/auto/telematik/ (visited on March 31, 2023)

Sahebi, S., and Nassiri, H. (2017). "Assessing Public Acceptance of Connected Vehicle Systems in a New Scheme of Usage-Based Insurance," *Transportation Research Record: Journal of the Transportation Research Board* 2625 (1), 62-69.

Schulmeyer, J. and Hess, T. (2022). "Towards an Understanding of Privacy Assurances – Literature Review and Research Agenda, " *PACIS 2022 Proceedings*. 59.

Seter, H., Hansen, L., and Arnesen, P. (2021). "Comparing user acceptance of integrated and retrofit driver assistance systems – A real-traffic study," *Transportation Research Part F: Traffic Psychology and Behaviour* 79, 139-156.

Shruthi, K., Ramaprasad, P., Ray, R., Naik, M. A., and Pansari, S. (2015). "Design of an anti-theft vehicle tracking system with a smartphone application," in: *2015 International Conference on Information Processing (ICIP)*, Pune, India, 755-760.

Śliwiński, A., and Kuryłowicz, Ł. (2021). "Usage-based insurance and its acceptance: An empirical approach," *Risk Management and Insurance Review* 24 (1), 71-91.

Smith, H. J., Dinev, T., and Xu, H. (2011). "Information privacy research: an interdisciplinary review," *MIS Quarterly* 35 (4), 989-1015.

Sokoll, C. S. (2021). *Certification in the Digital Age: Influence on Consumer Behavior*. Doctoral dissertation, Universität St. Gallen.

Soleymanian, M., Weinberg, C. B., and Zhu, T. (2019). "Sensor Data and Behavioral Tracking: Does Usage-Based Auto Insurance Benefit Drivers?" *Marketing Science* 38 (1), 21-43.

Spears, J. L. (2013). "The effects of notice versus awareness: An empirical examination of an online consumer's privacy risk treatment," in: *2013 46th Hawaii International Conference on System Sciences*, Maui, HI, USA, 3229-3238.

Sterk, F., Peukert, C., Hunke, F., and Weinhardt, C. (2022). "Understanding Car Data Monetization: A Taxonomy of Data-Driven Business Models in the Connected Car Domain," in: *Wirtschaftsinformatik 2022 Proceedings*, 7.

Stocker, A., Kaiser, C., and Fellmann, M. (2017). "Quantified Vehicles," *Business & Information Systems Engineering* 59 (2), 125-130.

Streich, M., D'Imperio, A., and Anke, J. (2018). "Bewertung von Anreizen zum Teilen von Daten für digitale Geschäftsmodelle am Beispiel von Usage-based Insurance," *HMD Praxis der Wirtschaftsinformatik* 55 (5), 1086-1109.

Swan, M. (2015). "Connected Car: Quantified Self becomes Quantified Car," *Journal of Sensor and Actuator Networks* 4 (1), 2-29.

Tax, S. S., Brown, S. W., and Chandrashekaran, M. (1998). "Customer Evaluations of Service Complaint Experiences: Implications for Relationship Marketing," *Journal of Marketing* 62 (2), 60-76.

Trager, J., Kalová, L., Pagany, R., and Dorner, W. (2021). "Warning Apps for Road Safety: A Technological and Economical Perspective for Autonomous Driving – The Warning Task in the Transition from Human Driver to Automated Driving," *International Journal of Human–Computer Interaction* 37 (4), 363-377.

Tsai, H. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., and Cotten, S. R. (2016). "Understanding online safety behaviors: A protection motivation theory perspective," *Computers & Security* 59, 138-150.

Tselentis, D. I., Yannis, G., and Vlahogianni, E. I. (2017). "Innovative motor insurance schemes: A review of current practices and emerging challenges," *Accident; analysis and prevention* 98, 139-148.

Tulusan, J., Staake, T., and Fleisch, E. (2012). "Providing eco-driving feedback to corporate car drivers," in: Dey, A. K., Chu, H.-H., & Hayes, G. (eds.) *Proceedings of the 2012 ACM Conference on Ubiquitous Computing - UbiComp '12*, Pittsburgh, Pennsylvania, USA, 212.

Uhlemann, E. (2016). "Connected-Vehicles Applications Are Emerging [Connected Vehicles]," *IEEE Vehicular Technology Magazine* 11 (1), 25-96.

Vance, A., Siponen, M., and Pahnila, S. (2012). "Motivating IS security compliance: Insights from Habit and Protection Motivation Theory," *Information & Management* 49 (3-4), 190-198.

Vavouranakis, P., Panagiotakis, S., Mastorakis, G., and Mavromoustakis, C. X. (2017). "Smartphone-Based Telematics for Usage Based Insurance," in: Mavromoustakis, C. X., Mastorakis, G., & Dobre, C. (eds.), *Advances in Mobile Cloud Computing and Big Data in the 5G Era*, Cham: Springer International Publishing, 309-339.

Wahlström, J., Skog, I., and Händel, P. (2017). "Smartphone-Based Vehicle Telematics: A Ten-Year Anniversary," *IEEE Transactions on Intelligent Transportation Systems* 18 (10), 2802-2825.

Walter, J., and Abendroth, B. (2018). "Losing a Private Sphere? A Glance on the User Perspective on Privacy in Connected Cars," in: Zachäus, C., Müller, B., & Meyer, G. (eds.*) Advanced Microsystems for Automotive Applications 2017*, Cham: Springer International Publishing, 237-247.

Walter, J., and Abendroth, B. (2020). "On the role of informational privacy in connected vehicles: A privacy-aware acceptance modelling approach for connected vehicular services," *Telematics and Informatics* (49), 101361.

Walter, J., Abendroth, B., Pape, T. von, Plappert, C., Zelle, D., Krauß, C., Gagzow, G., and Decke, H. (2018). "The user-centered privacy-aware control system PRICON," in *Proceedings of the 13th International Conference on Availability, Reliability and Security*, Hamburg, Germany1-10.

Wang, T., Duong, T. D., and Chen, C. C. (2016). "Intention to disclose personal information via mobile applications: A privacy calculus perspective," *International Journal of Information Management* (36:4), 531-542.

Wang, Y., and Herrando, C. (2019). "Does privacy assurance on social commerce sites matter to millennials?" *International Journal of Information Management* (44), 164-177.

Waskom, M. L. (2021). "seaborn: statistical data visualization," *Journal of Open Source Software* 6 (60), 3021.

Williams, L. J., and Abdi, H. (2010). "Fisher's least significant difference (LSD) test," *Encyclopedia of research design* 218 (4), 840-853.

Xu, H., & Dinev, T. (2022). "Guest Editorial: Reflections on the 2021 Impact Award: Why Privacy Still Matters," *MIS Quarterly* 46 (4), xx-xxxii.

Xu, H., Dinev, T., Smith, H. J., and Hart, P. (2008). "Examining the formation of individual's privacy concerns: Toward an integrative view," in *Proceedings of 29th International Conference on Information Systems*, Paris, France, 6.

Xu, H., Teo, H. H., Tan, B. C., and Agarwal, R. (2012). "Research note—effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services," *Information Systems Research* 23 (4), 1342-1363.

Zeng, F., Ye, Q., Yang, Z., Li, J., and Song, Y. A. (2022). "Which Privacy Policy Works, Privacy Assurance or Personalization Declaration? An Investigation of Privacy Policies and Privacy Concerns," *Journal of Business Ethics* 176 (4), 781-798.