Inter-regional Lens on the Privacy Preferences of Drivers for ITS and Future VANETs

Inter-regional Lens on the Privacy Preferences of Drivers for ITS and Future VANETs

Lejla Islami*
lejla.islami@kau.se
Karlstad University
Karlstad, Sweden

Agnieszka Kitkowska
agnieszka.kitkowska@ju.se
Jönköping University
Jönköping, Sweden

Simone Fischer-Hübner
simone.fischer-huebner@kau.se
Karlstad University
Karlstad, Sweden &
Chalmers University of Technology
Gothenburg, Sweden

ABSTRACT

Intelligent Transportation Systems (ITS) are on the rise, yet the knowledge about privacy preferences by different types of drivers in this context needs to be improved. This paper presents survey-based research (N = 528) focusing on preferences of drivers from South Africa and the Nordic countries for data processing and sharing by ITS, including future vehicular ad hoc networks. Our results indicate regionally framed drivers' privacy attitudes and behaviours. South African participants have higher privacy concerns and risk perception. However, their preferences to share location data with police, family and friends, emergency services, and insurance companies are higher. Moreover, the region significantly affects preferences for transparency and control and sharing frequency, as well as willingness to pay for privacy, which are higher among the South Africans. We discuss how our results on factors, including region, impacting drivers' privacy preferences can contribute to the design of usable privacy and identity management for ITS.

CCS CONCEPTS

• **Security and privacy → Human and societal aspects of security and privacy**; *Privacy protections*; *Usability in security and privacy*;

KEYWORDS

Intelligent transportation, vehicular communication, privacy preferences, cross-regional comparison, privacy-enhancing technologies (PETs)

ACM Reference Format:
Lejla Islami, Agnieszka Kitkowska, and Simone Fischer-Hübner. 2024. Inter-regional Lens on the Privacy Preferences of Drivers for ITS and Future VANETs. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '24), May 11–16, 2024, Honolulu, HI, USA.* ACM, New York, NY, USA, 20 pages. https://doi.org/10.1145/3613904.3641997

CHI '24, May 11–16, 2024, Honolulu, HI, USA

ACM ISBN 979-8-4007-0330-0/24/05
https://doi.org/10.1145/3613904.3641997

1 INTRODUCTION

Intelligent transportation systems (ITS), including navigation and other driver assistance apps, that are in use today as well as emerging and future vehicular communication systems, collect vast amounts of data, including detailed information about vehicles, their drivers and their locations. The future advancement of ITS in the form of Vehicular ad hoc networks (VANETs) comprising vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication will be fueled with a number of services for drivers to enhance driving safety and efficiency. These value-added services rely on collecting and processing location and driving data, which allows drawing inferences from driving behaviour and location patterns, including insights into drivers' social contacts and lifestyles, thus enabling the generation of comprehensive personal profiles of drivers.

Consequently, risks to the privacy of individuals may arise. Regulations, such as the EU General Data Protection Regulation (GDPR) [1] and other recently introduced privacy and data protection laws for different regions, including South African's Protection of Personal Information Act (POPI Act) [2], address such risks. However, given the amount and sensitive nature of collected data distinctive to ITS and to VANETs, regulations will by themselves not be sufficient to ensure privacy. Complementing means and technologies are needed to enforce privacy by design and implement usable privacy controls for users.

Already in 1968, Westin defined privacy as control—"the claim of individuals, groups and institutions to determine for themselves when, how and to what extent personal information about them is communicated to others [86]". As Duckham and Kulik [27] argue, Westin's definition also applies to the location data and therefore, control of location is a central element of location privacy. To empower drivers to control the processing and communication of their location data, usable systems enabling management of their digital identities and privacy permissions are needed for ITS including future VANETs. For designing usable privacy-preserving identity management systems, a thorough understanding of individuals' privacy preferences related to ITS will be a prerequisite.

As another definition for privacy, Nissenbaum proposed contextual integrity, describing contexts as social settings "characterized by canonical activities, roles and relationships, power structures, norms and internal values" [58]. According to this theory of contextual privacy, privacy perceptions may differ depending upon the type of shared data, the entity the data is shared with, its purpose of use, and more. The present study considers contextual integrity in

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679
[2] https://popia.co.za/

investigating location privacy preferences for ITS, including future VANETs. As the context, we investigate location sharing via ITS with different entities for various purposes. Moreover, our study investigates the impact of the users' regional backgrounds on their privacy preferences.

As discussed in [68], the common and unique cultural values of transparency, openness and trust presented in Nordic countries, and Hofstede's cultural comparisons, provide justification for considering the Nordic countries a fairly unified cultural region. Particularly, the Nordics are considered a unified cultural region considering openness value, rooted in the transparency of the governmental functioning [68, 83] and decision-making [46] and the principle of public accessibility of official records [37]. Other regional clustering provide further reasons for considering the Nordic societies a unified cultural environment. Gupta et al. [41] grouped 61 nations into ten cultural clusters and found that the Nordic cluster is characterized by strong practices of uncertainty avoidance, future orientation and institutional collectivism, and gender egalitarianism. Nordic region's cultural unity is also based upon similar psychological, sociological, demographic, and economic characteristics of nations as shown by other attempts to cluster societies [75, 88].

Previous research shows that privacy perceptions of drivers in ITS might be determined by regional background [43]. While past studies provide valuable insights regarding factors impacting users' behaviour and acceptance of ITS [3, 49, 63, 84], to our knowledge, previous cross-regional comparisons are limited and rarely focus on non-Western populations. Addressing this gap, we investigate the privacy preferences of drivers from South Africa and Nordic countries for ITS for controlling and sharing location data and preferences for privacy trade-offs with usability, safety, and cost. Comparing these two regions was partly motivated by differences in privacy traditions and regimes. Nordic countries were among the first to introduce data protection laws worldwide, in 2018, replaced by the GDPR. Such long traditions of data protection laws and modernised data protections introduced by the GDPR have strengthened individuals' rights and ensured accountability compliance. In contrast, South Africa's first privacy regulation (POPI Act) came into force in 2020, which means that South Africans have less experience with legal means for protecting their privacy. Moreover, differences in safety and rates of crime [52] motivated us to compare these regions, including car-related crimes (e.g. car hijacking) [77], that are significantly higher in South Africa and could impact the drivers' privacy preferences.

Past research indicates that privacy concerns significantly affect the intention to use connected vehicles [1, 72]. Similarly, preferences for control and transparency and privacy trade-offs depending upon the purpose of data use, privacy issues, and demographic and personal characteristics have been shown to affect attitudes and behaviours [2, 13, 73]. Moreover, risk perception may affect user behaviour and acceptance of ITS.

Therefore, the present research objective is twofold. First, through quantitative inquiry, we aim to explore whether the region impacts privacy perceptions and preferences for ITS to confirm findings from previous qualitative studies [42, 43]. Second, we aim to assess the relationship of latent constructs and demographics [3] with each other and their role in explaining drivers' privacy preferences for ITS. To achieve the objective, we raise the following research questions relating to the regions of South Africa and the Nordics and to ITS, including future VANETs.

RQ1 How do participants of different region, gender, privacy concerns, and risk perception differ in preferences for sharing location data for ITS?

RQ2 How do participants of different region, gender, privacy concerns, and risk perception differ in preferences for transparency and control, and sharing frequency?

RQ3 How do participants of different demographics (region, gender) differ in location privacy trade-off preferences for ITS?

To reach the objective, we conducted an online survey with 528 drivers from South Africa and Nordic countries (including Finland, Denmark, Sweden, Norway, and Iceland), investigating their preferences for ITS, including future VANETs. The analysis identified the potential behavioural consequences of privacy concerns, risk perceptions and regional background. Our findings show that the regional background significantly impacts the drivers' preferences for sharing and controlling location data in ITS and VANETs, including the preferences for privacy trade-offs with costs.

Our research findings can contribute to the future design of usable identity management systems for ITS users. To this end, our results provide valuable insights for defining and offering users suitable profiles of privacy settings, including regionally-dependent ones, that users can easily select after starting from a "privacy by default" profile. Moreover, insights into privacy factors and preferences for privacy controls that matter for users to different degrees can, in future, also serve as a basis for training Machine Learning (ML)-supported privacy assistants that predict and propose suitable individualised settings for those privacy controls that are of importance for ITS and VANET users. By this, our results can help address usability issues identified by prior studies that have shown that the number of settings is increasing significantly, often making their configuration less usable, and existing settings fail to capture users' privacy preferences accurately (see e.g.[76]).

As this study is among the few attempts (the first to our knowledge) to explore privacy preferences across these two regions, it can advance the theoretical understanding of cross-regional phenomena and their importance for introducing future regionally-dependent privacy-preserving identity management systems for ITS including VANETs.

2 BACKGROUND AND RELATED WORK

2.1 Privacy constructs and privacy models

Our work shares similarities with many previous attempts to quantify privacy attitudes and behaviour in the context of vehicular networks. Bella et al. [7] ran a large-scale survey to analyse privacy and trust perception in connected cars and found low privacy concerns from the drivers. They mainly attribute the results to perceived high trust in security that personal data is processed lawfully and respondents' lack of awareness of data collection. The same

[3] Note that we differentiate between the region and other demographics, such as gender or age groups. However, in some instances, demographics other than gender could not be used in the data analysis due to the unequal distributions.

methodical approach was used by Schmidt et al. [72, 73] in a series of studies to measure privacy perceptions and requirements for vehicle-to-everything technology. The effect of gender, age, type of data (vehicle- or driver-related), and prior experience with driver assistance systems influenced the propensity to share data. Koester et al. [49] investigated privacy risk perception in connected cars and its effect on willingness to share car data, and showed the need for cognition and institutional trust to moderate the effect of privacy risk on willingness to share. Acharya and Mekker [2] found perceived data privacy and security to lower the data sharing intention in connected vehicle technology.

Shifting the focus to the role of cultural bias on willingness to share personal information in connected autonomous vehicles, Anastasopoulou et al. [3] concluded that cultural bias may significantly impact willingness to share. However, their pilot study did not report any impact of perceived privacy risk on willingness to share personal data in connected autonomous vehicles.

The effect of drivers' privacy concerns, risk perception, or demographics on users' privacy preferences under different contexts still needs more investigation. For instance, previous work in different domains shows contradicting results regarding the importance of risk perception for predicting behavioural intention or willingness to share [3, 49, 63, 84]. On the other side, the prior studies reflect trust as a determinant of risk perceptions and privacy decision-making, which has also been established in the context of vehicular networks. In the present research, we do not investigate trust directly, assuming it is integral to the notion of region, as discussed in section 2.2. Moreover, we go beyond related work by conducting an inter-regional comparison of drivers' privacy preferences for ITS for controlling and sharing location data, including their preferences for privacy trade-offs of future Privacy Enhancing Technology (PET) solutions for VANETs with usability, safety, and cost.

2.2 Regional investigation

Culture is defined as the "ideals, values, and assumptions about life that are widely shared among a population ... that guide specific behaviour patterns" [22]. One crucial component of such a definition could be a geographical area— referred to in this paper as a region. Studies show that privacy preferences for vehicular systems differ across regions [43, 74]. Schoettle and Sivak [74] conducted a survey-based international study on public privacy opinion in the UK, US, and Australia. The results indicate a similar willingness to pay for connected vehicles across the three countries, with a considerable percentage of participants not willing to pay extra (45.5% in the US, 44.8% in the UK, and 42.6% in Australia) without specifying reasons for their hesitance. The respondents in the UK and Australia tended to be less concerned over data privacy than those in the US. Similarly, Cunningham et al. [15] showed that the Australian respondents do not express great concerns about data privacy for automated vehicles.

Due to the scarce research into the effects that regions might have on privacy preferences, the current study conducted an inter-regional survey, which, to the best of our knowledge, is the first survey employed in South Africa and Nordic countries in the context of VANETs.

2.3 Location sharing preferences

As previous studies showed, the willingness to share location information is context-dependent. It can e.g. depend on the number of locations that a user visits in a day [81], on the time of day, day of the week, or exact location [8] or whether data is shared with public or private entities, with law enforcement, or within a social network [13]. Moreover, [45] show that users are more willing to share personal information in informal settings. Our study is the first to investigate location sharing not only for the context of various entities with that location data is shared for various purposes, but also for the context of ITS and VANETS and in comparison for different regions including regions that have not been well studied yet.

2.4 Location privacy trade-offs

If technological services, such as ITS, rely on personal data, the user usually needs to value the service against some privacy trade-off, often evaluated through perceived benefits from the obtained services on the price of reduced privacy. The juxtaposition of benefits versus privacy risks of personal information disclosure is termed privacy calculus [14]. This theoretical construct assumes that when assessing the privacy trade-off, the decision to reveal personal information is made as users perceive that the gains outweigh the potential privacy concerns. In a study by Cottrill et al. [13], the relationship between willingness to trade location information and utility in vehicular context is explained regarding reduced costs, travel time, and safety benefits.

For example, in Schmidt et al. [72], the drivers' evaluation of benefits and the privacy loss in connected vehicles are addressed in terms of traffic safety, efficiency, costs and comfort.

Privacy and usability trade-offs also need to be addressed with privacy-enhancing location-based service (LBS) architectures [24, 44, 55], including technical approaches providing k-anonymity [70]. The user of LBS would have to trade between service accuracy and location inaccuracy, as privacy is at odds with usability in this case.

Other trade-offs have also been addressed in the context of vehicular technologies. For instance, Derikx et al. [23] used conjoint analysis to test how consumers of car insurance companies value privacy against monetary benefits. Their results imply that consumers prefer their current insurance products to usage-based car insurance due to privacy concerns. However, they showed that minor financial compensations overcame privacy concerns. Poikela and Toch [63], investigated users' valuation of location privacy in several one-time sharing scenarios in crowdsourcing systems. The results indicate that the amount of money offered for sharing a location was a significant factor in the decision to share a location. Other studies have tackled the cost trade-off, and participants reported the compensation they would need to have their location monitored [10, 16, 19].

Unlike the related work, the current study focuses on privacy trade-offs of PET solutions for future VANETs with usability, and cost from the drivers' perspective. Moreover, by approaching the usability trade-off of location privacy from the users' viewpoint, our work differs from previous studies, which take a technical approach.

3 METHOD

3.1 Questionnaire development

Based on the results of prior interview studies [42, 43], we developed an online survey designed to examine drivers' privacy preferences for current ITS and future vehicular communication systems. We decided to use the survey instrument as it is commonly used in privacy research, and it is feasible to measure privacy constructs, such as privacy attitudes and perspectives [64].

The constructs measured in our study are privacy concerns, risk perception, preferences for transparency and control, preferences for sharing location data (RQ1, RQ2), and preferences for usability and cost trade-offs with privacy (RQ3). Each construct was measured with multiple Likert items. The questionnaire contains self-developed privacy scales. When possible, to improve accuracy and content validity (relevance and representativeness of the instrument's content), instruments acquired from past research are in use.

The survey can be divided into five parts, as follows (Figure 1 provides an overview of the study order):

Part I Participants were first presented with the consent form providing information regarding their data subject's rights under the GDPR. After participants agreed to our consent form, we asked them to imagine using an Intelligent Transportation System that captures their location data (see Appendix Part I). We relied on the short description of current and future privacy-enhancing systems for VANETs, an explanation of key terms and illustrations of both systems, as well as privacy trade-offs of future VANETs through visualization. Additionally, in this part of the survey, the participants were given a short introduction to Intelligent Transportation Systems and future vehicular communication, including examples of the latter's functionality and an explanation of key terms such as location data and short-term pseudonyms.

Part II Next, we asked participants about their privacy concerns, risk perceptions in ITS and future VANETs, and preferences for transparency and control (for details, see Appendix Part II). Location privacy concerns (3 items) were measured using an existing scale from Walter and Abendroth [84]. The questions in this scale were modified to suit the present study better. Specifically, we asked regarding location information instead of personal information and changed the context to ITS instead of the service provider. Next, we used the risk perception (6 items) scale adopted from Poikela and Toch [63] to assess the drivers' perceived risk in the context of ITS. This was followed by a scale measuring preferences for control and transparency. We used a self-developed instrument (4 items) to measure drivers' willingness to manage and control location data as well as their desire to be informed about data collection and the purpose of use and profiling.

Part III In this part of the survey, we measured preferences for sharing location data (8 items), reflecting the willingness of participants to share location data with different entities for specific purposes, as well as the frequency of sharing the location data (for details, see Appendix Part III). The set of items in this part of the survey provides a granular identification of purposes for which drivers are willing to disclose location data with entities such as family, friends, government, police, other car drivers, insurance companies and emergency services.

Part IV The next part of the survey consisted of asking participants about their preferences regarding privacy trade-offs of PET solutions with future VANETs with usability and costs (for details, see Appendix Part IV). The respondents were presented with two scenarios to help them envision the privacy benefits of future vehicular systems, which are often at odds with privacy goals. As such, the scenarios assessed their willingness to trade privacy for usability benefits and willingness to pay for privacy-preserving solutions with short-term pseudonyms to protect their location data.

- *Cost trade-off scenario.* We asked participants to envision using a privacy-preserving solution, making it harder for the system to identify someone and see their exact location. To achieve that, future systems for VANETs will use pseudonyms instead, which are identifiers other than someone's real name [62]. As the different uses of the same pseudonym can be linked to each other and could also relate to someone's real identity, the usage of short-term pseudonyms is employed, which are pseudonyms that are changed frequently to make it harder for the other car drivers or the service provider to identify someone. However, the constant changing of pseudonyms incurs more costs for obtaining signed pseudonyms from an issuing party. Hence, a trade-off between privacy and costs can be made dependent on how frequently the pseudonyms are changed. We asked participants whether they were willing to pay more to hide their location and to what extent.
- *Usability trade-off scenario.* We asked the participants to envision the navigation application searching for available parking spots nearby. In the first navigation map (Figure 2 A), the user is shown the parking places in the specific street they are interested in. In this case, they are the only driver in the area, and they can be easily identified. The second map (Figure 2 B) represents a more privacy-friendly solution that applies the concept of k-anonymity [70] to location privacy. Such k-anonymous location-based services, as presented in Gedik and Liu [34], Gruteser and Grunwald [39] get less detailed location data from the drivers, and hence, they can not be easily identified. This is because they are searching for parking places for a larger region instead, and since at the time when the location data is collected, there are at least k other drivers in the area (who all share their locations), that location cannot uniquely identify the driver. However, this option offers a lower level of usability in that the user would have to zoom in on the map and find their way to the parking places in the preferred street, leading to a privacy vs. usability trade-off.

  This k-anonymous location privacy scenario illustrating a privacy-usability trade-off is meaningful if parking spaces on either a smaller or greater area map are directly displayed by 3rd party location-based service (LBS). If a driver

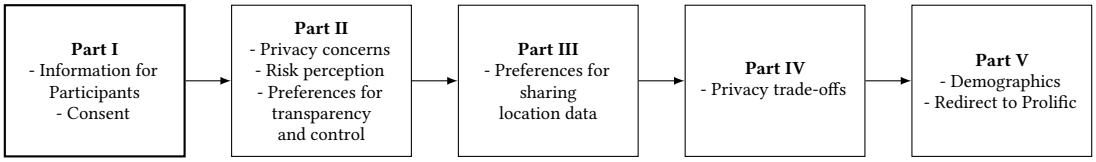

Figure 1: Overview of the study order.

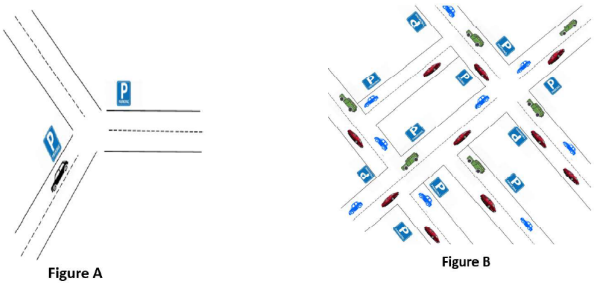

Figure 2: Maps illustrating the usability trade-off that needs to be made for a privacy-enhanced (k-anonymous) navigation application (Figure B) vs. a non-privacy-enhanced version (Figure A).

uses a local navigation application that knows their exact location, the app could, if it receives the free parking spaces information on a greater area map from the LBS, still show only the nearby parking places to the driver. Nonetheless, privacy-usability trade-off decisions, as illustrated by the scenario, may still need to be made if future VANET users decide to utilise peer-to-peer communication with other drivers in close proximity to ask for advice on free parking places close to a location of interest. Due to technical limitations, peer-to-peer communication in VANETs is only possible with close-by drivers and thus k-anonymity could not be assured (apart from the problem that drivers may even directly see each other's cars and link the car driver with the parking location of interest). Hence, drivers have to trade privacy for usability if they decide to ask peer drivers for advice. We asked participants whether they were willing to share their exact location for usability (as provided by the map in Figure 2 A).

(1) Demographics were addressed in the last part of the survey. We asked participants about their nationality, age, gender, level of education, and employment status. Next, we thanked the participants for taking part in the study and redirected them to Prolific.

Before running the study, we pilot-tested the survey with 10 participants to check the study's comprehensibility and usability. The results from the pilot tests confirmed that the study does not require further revisions.

3.2 Participants and data collection

We recruited 543 participants through Prolific, a commonly used online platform for recruiting participants for user studies. The answers were stored using pseudonyms in the form of participants' Prolific IDs, which were then removed after participants were paid to ensure data minimization. Participants were paid according to the standards of Prolific payments, 11.7 GBP per hour. The reason for choosing Prolific is that data processing in their platform is performed within a country (UK) that applies GDPR rules and provides an adequate level of data protection according to the EU Commission's adequacy decision from 2021. Moreover, previous studies have shown high reliability of the responses in Prolific compared to other crowd-sourcing platforms [61].

The prerequisites for taking part in the study were having a valid driving license and having used or using current ITS as well as speaking English. The reason for filtering participants in terms of language lies in the fact that English is the second language in South Africa and in Nordic societies, people are proficient in English [31]. Besides that, we decided to have the survey in English as it is hard to explain different technical terms (e.g., pseudonymity, linkability) in other languages. All the questions in the survey were compulsory, so we did not have any missing data. However, we eliminated the respondents who gave contradictory answers (for instance, they answered they were willing to pay for pseudonyms, but when asked to what extent, they chose the option of not to pay or vice versa, or completed the survey in a shorter time from what was considered the minimum amount of time (four minutes) to read it through). We excluded 15 respondents and selected the data from 528 respondents, of which 265 were from South Africa, and 263 were from the Nordics. Among the Nordic participants, 109 were from Sweden, 33 were from Norway, 40 were from Denmark, 68 were from Finland, and 13 were from Iceland.

The sample group consisted of mainly young adults of age ranges 18-24 (N = 104), 25-34 (N = 259), 35-44 (N = 111), 45-54 (N = 37), 55-64 (N = 13) and +65 (N = 4). 50.6% of the respondents identified themselves as females, 48.1% as males, and 1.3% as other non-binary. 0.9% had an education lower than high school, 32.4% had high school or professional qualification, 48.1% had a bachelor's degree, 15% had a master's degree, 2.3% a doctoral degree, and 1.3% preferred not to disclose their level of education. When asked about their employment status, 69.9% reported being employed, 8.9% were unemployed, 18.2% were students, 0.9% were retired and 2.1% preferred not to answer. See Table 1 for detailed demographics. Finally, 44.1% of the participants reported using Intelligent Transportation Systems (ITS) or navigation applications; most commonly used were built-in navigation systems in the car, Waze, TomTom, Garmin, CoPilot GPS, Magic Earth, Sygic GPS, car trackers, and Google Maps.

3.3 Ethical vetting

This study was conducted with the approval of the ethical advisor at Karlstad University. In accordance with the ethical requirements,

Table 1: Descriptive statistics of survey respondents (N = 528). SA - South Africa; NO - Nordics.

Demographics		Region (n)		Total	
		SA	NO	N	%
Gender	Female	154	100	254	48.1
	Male	110	157	267	50.6
	Other	1	6	7	1.3
Age	18-24	48	56	104	19.7
	25-34	149	110	259	49.1
	35-44	48	63	111	21.0
	45-54	13	24	37	7.0
	55-64	5	8	13	2.5
	65+	2	2	4	0.8
Education	Less than high school	1	4	5	0.9
	High school or professional qualification	80	91	171	32.4
	University degree	164	90	254	48.1
	Master's degree	16	63	79	15.0
	Doctorate degree	2	10	12	2.3
	Prefer not to say	2	5	7	1.3
Employment	Employed	201	168	369	69.9
	Unemployed	23	24	47	8.9
	Student	34	62	96	18.2
	Retired	2	3	5	0.9
	Prefer not to say	5	6	11	2.1
Country of residence	South Africa	–	–	265	50.2
	Sweden	–	–	109	20.6
	Iceland	–	–	13	2.5
	Finland	–	–	68	12.9
	Denmark	–	–	40	7.6
	Norway	–	–	33	6.3

we excluded exposing participants to any kind of emotional, physical, or health risk, avoided collecting any sensitive personal data, and the data was collected in a pseudonymised form and securely protected from unauthorized access. For the purpose of data minimization, the personal data collected was limited to the country of residence, age, gender, and education. Participation was voluntary, informed consent was obtained from the participants, and GDPR compliance was assured. Participants were reimbursed via the Prolific platform based on payments recommended by the platform. Likewise, the conducted data analysis was also anonymized.

4 RESULTS

In this section, we first report the reliability and validity of the scales used in the questionnaire. Next, we present the results of the statistical tests applied to answer the research questions.

Although our study is not based on experimental design and we do not manipulate any variables, we treat the study design as between-subject because of the categorical independent variables (gender, region) used in the statistical models. We chose the methods for data analysis following the recommendation from [80]. When appropriate, we applied analysis of variance since it is recommended when comparing populations [67]. Considering the RQ1, we used MANCOVA because of multiple dependent and mixed predictor variables (categorical and continuous). Applying MANCOVA was also driven by a probe for possible interactions between the independent categorical predictors. However, the results of MANCOVA are further explained with single regression models when assessing the effects of covariates on the different dimensions of preferences for sharing. We used regressions and non-parametric tests when appropriate to answer the remaining research questions. Also, as the main focus of the paper was to assess inter-regional differences and not the effects that privacy concerns and risk perceptions had on dependent variables, the latent constructs are independent variables for RQ1 and RQ2 but for RQ3.

While planning data analysis, the sample estimation was challenging, mainly because of the selected data analysis method—multivariate analysis of covariance. Hence, using G*Power, we estimated the sample size for ANCOVA with interactions—approximately 500 (with small effect size, α = .05, and power .95).

4.1 Instruments used in the study

To increase the reliability and validity of this work, we utilized, when applicable, existing scales developed by previous research. Prior acquired validated instruments were used to measure the latent variables: privacy concerns and risk perception. To assess reliability, we applied Cronbach's α estimate, looking for scores higher than 0.7 [36]. We checked whether previously developed scales' items load correctly using principal component analysis (PCA). The newly created scales measuring preferences for control

Table 2: Means of the variables (N = 528)

Construct	*M*	*SD*
Privacy concerns	3.64	1.01
Risk perception	3.41	0.92
Preferences for transparency and control	4.13	0.67
Preferences for sharing frequency	2.81	0.93
Sharing with government	3.25	1.07
Sharing with family and close friends	3.28	0.94
Sharing for emergency purposes	4.50	0.59
Sharing with insurance companies	2.91	1.08
Sharing with emergency services	3.84	0.90
Sharing with police	3.71	1.06
Sharing with other drivers	3.83	0.88

and transparency, and preferences for sharing location data were also evaluated and validated using Cronbach's α, PCA or the exploratory factor analysis (EFA) in the case of the scale measuring preferences for sharing location data. All items used to measure preferences for sharing location data, their loadings and Cronbach α values are represented in the Appendix Exploratory Factor Analysis, Table 6. The responses for the location privacy concerns construct, as well as for risk perception, preferences for transparency and control and preferences for sharing location data, were measured with fully labelled 7-point Likert items, anchored from 1 (*Strongly disagree*) to 7 (*Strongly agree*).

The means for each construct are listed in Table 2. We used the means in further analysis to determine the relationships with latent factors and explore demographics.

Privacy concerns. We run the PCA to check whether the items load correctly. All items loaded into a single factor, as expected, accounting for 84.43% of explained variance. The Kaiser-Meyer-Olkin (KMO) measure was good, .74, and Barlett's Test of Sphericity was significant, $p < .001$. We determined the reliability of this measurement as excellent, based on overall Cronbach's $\alpha = .91$. To compute the privacy concerns variable, we used means.

Risk perceptions. All six items loaded into one factor based on PCA, as anticipated, explaining 61.92% of the variance, with KMO = .89 and Barlett's Test of Sphericity at $p < .001$. The reliability of the measurement was good, Cronbach's $\alpha = .87$ and it would not have increased if any of the six items had been removed from the scale. The variable was computed based on the means.

Preferences for control and transparency. The results of the PCA were satisfying, with KMO = .64 and Barlett's Test of Sphericity at $p < .001$. As Cronbach's $\alpha = .74$ was above the commonly accepted threshold, we computed the preferences for transparency and control variable.

Preferences for sharing frequency. The PCA for this measurement resulted in one factor, as expected, accounting for 56.59% of the explained variance. The KMO was .68, and Barlett's Test of Sphericity was significant, $p < .001$. The internal consistency of this measurement was acceptable ($\alpha = .78$). We used means to compute the variable.

Preferences for sharing location data. We checked the scale's reliability and validity using EFA. We run EFA because it allows us to identify factors that explain the correlation between measured variables without requiring underlying theoretical processes [66]. The KMO (.92) and Barlett's Test of Sphericity (significant, $p < .001$) confirmed the suitability of EFA. We applied oblique rotation, oblimin and extracted seven factors based on Principal Axis Factoring (PAF). From the original 31 items, 30 remained after removing one item with commonality and loading < .3. The scree plot analysis and parallel analysis, indicated seven factors, identifying drivers' preferences for sharing location data: *sharing for emergency purposes in case of accidents, sharing with the police, sharing with the government, sharing with family and close friends, sharing with insurance companies, sharing with other drivers* and *sharing with emergency services*. We computed the internal consistency of this instrument based on the extracted factors, and Cronbach's alpha scores were all above .7. Appendix Exploratory Factor Analysis, Table 6 presents the items loading into each of the seven factors.

4.2 Descriptive Analysis

To understand the relationships between continuous variables, we examined correlations before conducting more complex data analysis to answer research questions. We checked the assumptions for the Pearson correlation test, which were good, apart from slight violations of normality, acceptable in large samples. The test results revealed mostly medium correlations between the variables. Table 3 presents the correlations between variables. There is a strong, significant positive relationship between risk perception and privacy concerns ($r = .70$, $p < .01$) and a positive moderate relationship between risk perception and preferences for transparency and control ($r = .46$, $p < .01$). There are small to moderate, significant negative correlations between privacy concerns and preferences to share location data with different entities such as the government (r = -.31, $p < .01$), police (r = -.23, $p < .01$), other drivers (r = -.15, $p <$ .01), emergency services (r = -.19, $p < .01$) and insurance companies (r = -.19, $p < .01$). This finding indicates that the more concerned drivers are about their location data, the less willing they might be to share it with different entities, and vice versa. Similarly, higher perceptions of risk are related to lower preferences for sharing, as indicated by the negative correlations. The medium to large positive correlations between the sharing preferences indicate that drivers share similar preferences for sharing location data with different entities such as government and police, emergency services, and other drivers.

4.3 Preferences for sharing location data

To assess the relationship between the latent variables, region, demographics, and the preferences for sharing **(RQ1)**, we applied multivariate analysis of covariance (MANCOVA). We included four covariates: privacy concerns, risk perception, transparency and control preferences, and sharing frequency to further improve the research model by measuring their effect on preferences for sharing location data. We considered correlations when selecting the appropriate test (univariate or multivariate). It is suggested that low correlations indicate that variables should be analyzed alone (univariate models), while moderate correlations indicate that variables should be analyzed in a model (multivariate) [21]. Hence, moderate correlations between the dimensions of preferences for sharing (Table 3) imply that multivariate analysis of covariance

Table 3: Correlations between variables: privacy concerns (PCS), risk perception (RPC), preferences for transparency and control (PTC), preferences for sharing frequency (FRQ), preferences for sharing location data with government (GOV), with family and friends (FFR), for emergency purposes (EMG), with police (POL), with other drivers (DRV), with emergency services (ESV) and with insurance companies (INS).

	PCS	RPC	PTC	FRQ	GOV	FFR	EMG	POL	DRV	ESV	INS
PCS	1	.70**	.43**	.31**	-.31**	-.10*	-.07	-.23**	-.15**	-.19**	-.19**
RPC		1	.46**	.32**	-.28**	.05	-.05	–.15**	-.17**	-.14**	-.04
PTC			1	.08	-.15**	.02	.17**	-.06	.03	-.04	-.06
FRQ				1	-.43**	-.18**	-.19**	-.37**	-.35**	-.39**	-.33**
GOV					1	.30**	.20**	.70**	.54**	.61**	.52**
FFR						1	.29**	.31**	.32**	.31 **	.42**
EMG							1	.30**	.41**	.42**	.16**
POL								1	.52**	.62**	.55**
DRV									1	.53**	.34**
ESV										1	.45**
INS											1

Note: Significance levels: *p < .05 and **p< .01.

is appropriate to study drivers' preferences for sharing location data as one construct. We checked the test's assumptions, such as outliers (Mahalanobis distance), linearity, multicollinearity (correlation test), univariate and multivariate normality, homogeneity (Box's M and Levene's test), and homoscedasticity (scatterplots). Levene's test of equality of variances was good ($p > .05$). Box's M of equality of covariance matrixes was insignificant ($p = .019$); hence, for the results of MANCOVA, we interpret Wilks' Lambda as a criterion (Table 4). Considering the demographics, we could not include demographics other than gender in the model. We were interested in looking for an interaction effect between the two categorical independent variables: region and gender. However, adding gender to the model had no effect ($p = .13$). Hence, the final model comprises one independent variable, region, and four covariates: privacy concerns, risk perception, preferences for transparency and control and preferences for sharing frequency.

Effects of covariates. Privacy concerns ($\eta_p^2 = .05$), risk perceptions ($\eta_p^2 = .04$), preferences for transparency and control ($\eta_p^2 = .07$) and preferences for sharing frequency ($\eta_p^2 = .17$) were significant adjustors of the combined dependent variables. We used individual ANCOVAs to examine their association. Particularly, privacy concerns significantly influenced single outcome variables: sharing with government ($\eta_p^2 = .02$), sharing with family and close friends ($\eta_p^2 = .02$), sharing with insurance companies ($\eta_p^2 = .03$), sharing with emergency services ($\eta_p^2 = .01$) and sharing with police ($\eta_p^2 = .02$). These variables correlated significantly (Table 3). Risk perceptions had a significant influence only on sharing with family and close friends ($\eta_p^2 = .01$). However, no significant correlation between these two variables suggests that risk perceptions might be a weak influencer of preferences for sharing with family and close friends.

Preferences for transparency and control was a significant adjustor of sharing for emergency purposes ($\eta_p^2 = .04$), sharing with insurance companies ($\eta_p^2 = .01$), and sharing with other drivers ($\eta_p^2 = .01$). Finally, there was a significant effect of preferences for sharing frequency on preferences for sharing with government ($\eta_p^2 = .13$), sharing with family and close friends ($\eta_p^2 = .02$), sharing for emergency purposes ($\eta_p^2 = .02$), sharing with insurance companies ($\eta_p^2 = .08$), sharing with police ($\eta_p^2 = .10$), sharing with emergency services ($\eta_p^2 = .12$) and sharing with other drivers ($\eta_p^2 = .10$). These variables correlated significantly (Table3).

Effects of independent variable. The regional background had a significant effect on combined dependent variables ($\eta_p^2 = .21$), particularly on sharing with family and close friends ($\eta_p^2 = .08$). There was a significant difference in the means of the two regional groups on sharing with family and friends. The scores for sharing with family and friends were higher among the South African participants ($M = 3.57$, $SD = 0.85$) than among participants from the Nordic countries ($M = 2.99$, $SD = 0.95$, 95% CI[0.40 - 0.73]), meaning that the former were more willing to share with family and friends than the latter. The impact of the region was significantly stronger when it comes to sharing with insurance companies ($\eta_p^2 = .13$); the univariate test confirmed that groups differed significantly in sharing with insurance companies. Participants from South Africa showed higher preferences for sharing with insurance companies ($M = 3.28$, $SD = 1.04$) than participants from Nordic countries ($M = 2.54$, $SD = 0.98$, 95% CI[0.62 - 0.97]). Further, the analysis identified the significant effect of region on sharing with emergency services ($\eta_p^2 = .01$) and on sharing with police ($\eta_p^2 = .01$). The mean scores were higher among South Africans ($M = 3.93$, $SD = 0.89$) than among the Nordics ($M = 3.75$, $SD = 0.91$, 95% CI[0.05 - 0.36]) for sharing with emergency services and sharing with the police, respectively, ($M = 3.81$, $SD = 1.03$), ($M = 3.61$, $SD = 1.09$, 95% CI[0.07 - 0.43]). Again, the results imply that South Africans were more willing to share location data with emergency services and police than the Nordic participants. Table 4 presents the details of the multivariate and univariate analyses.

Since we found slight violations of normality when inspecting the data, we also ran nonparametric analyses to test the effects. A series of Mann-Whitney U tests corroborate the results further: it revealed a significant effect of the region on preferences for sharing ($p < .05$).

4.3.1 Influence of covariates on preferences for sharing. We identified all four covariates as significant adjustors of the preferences for sharing in the main MANCOVA model. To understand how these

Table 4: MANCOVA: effects of region (REG) on dependent variables: sharing with government (GOV), sharing with family and friends (FFR), sharing for emergency purposes (EMG), sharing with insurance companies (INS), sharing with emergency services (ESV), sharing with police (POL), and sharing with other drivers (DRV).

	Multivariate		Univariate						
			F(1,522)						
	Wilks's lambda	F(7,516)	GOV	FFR	EMG	INS	ESV	POL	DRV
Covariates									
PCS	0.95	4.00***	7.82**	12.41***	2.02	16.56***	4.55*	10.33**	0.33
RPC	0.96	2.80**	0.61	6.19*	0.79	3.42	0.10	0.45	1.81
PTC	0.93	5.19***	0.70	0.56	21.98***	3.91*	< .01	0.01	6.23*
FRQ	0.83	15.28***	76.33***	12.71***	12.76***	47.35***	68.51***	58.78***	55.87***
Fixed factors									
REG	0.79	19.40***	0.46	45.93***	1.40	80.93***	6.90**	7.13**	0.42

Note: Significance values are based on *p <.05, **p <.01 and ***p< .001.

factors jointly influenced each of the preferences for sharing **(RQ1)**, we performed a series of simultaneous multiple regression analyses on all four covariates and our independent variable: regional background. The single dependent variables in the regression models are the dimensions of the preferences for sharing independently: sharing with government, sharing with family and close friends, sharing for emergency purposes, sharing with insurance companies, sharing with police, sharing with other drivers and sharing with emergency services.

First, we checked the assumptions for regression: linearity (scatterplots), multicollinearity (with tolerance values above .4 and VIF values between 1 and 2.5), and homoscedasticity. All models were significant ($p < .001$). The detailed results of the seven regression models are presented in Table 5.

- Privacy concerns and preferences for sharing frequency were found to statistically significantly affect preferences for sharing with the government. Overall model's predictive value was $F(5, 522) = 29.67$, adjusted $R^2 = .21$.
- Regarding preferences for sharing with family and close friends, privacy concerns, risk perceptions, preferences for sharing frequency, and region jointly influenced the outcome variable, with the overall model $F(5, 522) = 17.82$, adjusted $R^2 = .14$.
- Corroborating the MANCOVA model, preferences for sharing frequency and preferences for transparency and control were found to be significant predictors of the preferences for sharing for emergency purposes with the overall model $F(5, 522) = 9.12$, adjusted $R^2 = .07$.
- In the sharing with insurance companies model, there were four significant predictors of the dependent variable: privacy concerns, preferences for sharing frequency, region and preferences for transparency and control. The overall model value was $F(5, 522) = 36.64$, adjusted $R^2 = .25$.
- Privacy concerns, preferences for sharing frequency, and region were the significant predictors of preferences for sharing with emergency services, with the model's predictive value $F(5, 522) = 21.41$, adjusted $R^2 = .16$.
- Privacy concerns, preferences for sharing frequency and region were significantly predicting the preferences for sharing with police. Overall model's predictive value was $F(5, 522) = 21.60$, adjusted $R^2 = .16$.
- There were only two significant predictors of preferences to share with other drivers: preferences for sharing frequency and preferences for transparency and control, with the overall model value $F(5, 522) = 16.79$, adjusted $R^2 = .13$.

The results indicate that as privacy concerns increase, the drivers' willingness to share location data with the government, police, family and friends, insurance companies, and emergency services decreases. Furthermore, the higher drivers' perceived risk, the higher their preferences to share location data with family and friends. Conversely, the more positive drivers feel about transparency and control concerning third parties, such as insurance companies and other drivers, the more willing they are to share location data. Additionally, these results were yet another confirmation that frequency of sharing—how often location is shared when driving and the granularity of it—is strongly related to drivers' willingness to share.

4.3.2 Relationship between region and internal factors. To better understand our findings regarding the preferences for sharing, we have also looked separately at the relationships between the region and internal factors **(RQ1)** using a t-test. We tested the assumptions for the independent samples t-test, and both the normality assumption and the assumption of equal variances were slightly violated. However, since the Welch t-test is robust against the violation of normality in large sample sizes, we run it. There were significant effects of region on privacy concerns ($t(524.84) = 4.90$, $p < .001$, Cohen's $d = .43$) and risk perceptions ($t(518.59) = 8.73$, $p < .001$, Cohen's $d = .76$). The Welch t-test showed a significant difference in privacy concerns between the two groups with South Africans scoring higher ($M = 3.85$, $SD = 0.97$) than Nordics ($M = 3.43$, $SD = 1.01$). A significant regional difference was also found regarding risk perceptions. Especially, South African drivers ($M = 3.74$, $SD = 0.81$) perceived higher risk than the Nordic drivers ($M = 3.09$, $SD = 0.91$).

To validate the results further, we also ran the non-parametric Mann-Whitney U test as the assumption of equal distributions was

Table 5: Joint influence of privacy concerns (PCS), risk perception (RPC), preferences for sharing frequency (FRQ), preferences for transparency and control (PTC) and region (REG) on dependent variables: sharing with government (GOV), sharing with family and friends (FFR), sharing for emergency purposes (EMG), sharing with insurance companies (INS), sharing with emergency services (ESV), sharing with police (POL), and sharing with other drivers (DRV).

	GOV		FFR		EMG		INS		ESV		POL		DRV	
	β	r_p	β	r_p	β	r_p	β	r_p	β	r_p	β	r_p	β	r_p
PCS	-.16**	-.12	-.21***	-.15	-.09	-.06	-.22***	-.18	-.12*	-.09	-.18**	-.14	-.03	-.03
RPC	-.05	-.03	.15*	.11	-.06	-.04	.11	.08	.02	.01	.04	.03	-.08	-.06
FRQ	-.36***	-.36	-.16***	-.15	-.16***	-.15	-.28***	-.29	-.36***	-.34	-.33***	-.32	-.33***	-.31
PTC	-.04	-.04	-.04	-.03	.23***	.20	-.09*	-.09	<.01	<.01	<-.01	<-.01	.12*	.11
REG	-.03	-.03	-.30***	-.28	-.05	-.05	-.37***	-.37	-.11**	-.11	-.12**	-.12	.03	.03

Note: Significance values are based on *p<.05, **p<.01 and ***p<.001; β (beta) refers to the standardized regression coefficient.

slightly violated. The Mann-Whitney U test confirmed that privacy concerns were greater for South Africans (*Mdn* = 4.00, n = 265), compared to Nordics (*Mdn* = 3.66, n = 263), U = 25674.00, $p < .001$, with a small effect size r = -.23. Similarly, South African drivers (*Mdn* = 3.83, n = 265) showed higher perceptions of risk than their counterparts from the Nordic countries (*Mdn* = 3.00, n = 263), U = 20345.50, with a medium effect size r = -.36.

4.4 Preferences for transparency and control, and sharing frequency

Considering demographics, because of the unequal distribution (e.g., low numbers of participants from certain age groups), demographic comparisons were sometimes difficult to conduct. However, having a sample balanced around the gender (excluding the seven participants who selected "Other" answering the gender question), we used parametric tests to assess potential significant differences.

We used a t-test to assess differences in privacy concerns and risk perceptions among males and females **(RQ2)**. We found a significant effect of gender on risk perceptions (t(514.16) = -2.63, $p = .009$), indicating that females ($M = 3.53$, $SD = 0.84$) perceived higher risk than males ($M = 3.32$, $SD = 0.97$). There was no effect on privacy concerns.

We used regression analysis to investigate preferences for transparency and control, and sharing frequency. Before the analysis, we checked regression assumptions, such as linearity, homoscedasticity and multicollinearity. To check for linearity, we looked at scatterplots. To assess multicollinearity, we looked at the tolerance values, which were above .4, and VIF values, which were between 1 and 2.5.

We run bootstrapped regression analysis to study the preferences for transparency and control **(RQ2)**. The dependent variable in the model is preferences for transparency and control. The independent variables were privacy concerns, risk perception, gender and regional background. We decoded the dichotomous variables into dummy variables in order to assess differences in regional and gender groups. The model resulted in a significant change in the F ratio ($p < .001$). South African region ($\beta = .14$), privacy concerns ($\beta = .21$) and risk perceptions ($\beta = .28$) were found to statistically significantly affect preferences for transparency and control ($p < .001$). Overall model's predictive value was $F(4, 516) = 44.68$, adjusted $R^2 = .25$. We found gender did not significantly affect preferences for transparency and control ($\beta = -.04$, $p = .33$).

We run a bootstrapped regression analysis to investigate preferences for sharing frequency **(RQ2)**. Our independent variables were region, gender, privacy concerns and risk perceptions. We created dummy variables for representing the categories in the predictor variables: gender and region. The overall model resulted in a significant change in the F ratio ($p < .001$) with predictive value $F(4, 516) = 19.57$, adjusted $R^2 = .13$. There were three significant predictors of preferences for sharing frequency: South African region ($\beta = -.15$, $p < .001$), privacy concerns ($\beta = .16$, $p < .01$) and risk perceptions ($\beta = .25$, $p < .001$). Again, gender did not significantly predict preferences for sharing frequency ($\beta = .06$, $p = .16$).

4.5 Preferences for privacy trade-offs

To answer the **RQ3**, we used non-parametric tests. We ran the Chi-Square Test of Independence to analyze whether participants' preferences for trade-offs were represented across the two regional groups and demographics (gender). The results showed that there was a significant difference, $X^2 = 23.78$, $df = 1$, $p < .001$ in drivers' willingness to pay for pseudonyms by region. Such findings indicate that South African drivers were more willing to pay for pseudonyms than drivers from Nordic countries. There was no significant evidence of the association between usability trade-off and regional background.

A Chi-Square test showed a significant difference in drivers' preferences for cost trade-off by gender $X^2 = 4.59$, $df = 1$, $p = .032$, with females showing higher preferences for paying compared to males. The X^2 test results showed again a significant difference, $X^2 = 9.85$, $df = 3$, $p = .020$, in preferences for usability trade-off by gender. Crucially, these results demonstrated that the choice of usability over privacy was more frequent among males than females (more than twice as frequent). Lastly, the results were insignificant regarding preferences for trade-offs across different age groups, levels of education, and levels of employment.

5 DISCUSSION

The results of the present study show that the latent constructs (privacy concerns and risk perceptions), preferences for transparency and control, preferences for sharing frequency, and region affect the preferences for sharing location data with different entities (RQ1). The results also revealed that the preferences for sharing with different entities such as family and close friends, insurance companies, emergency services and police were higher for South Africans than for the Nordics (RQ1).

Moreover, the latent constructs— privacy concerns, risk perceptions and regional background impact preferences for transparency and control and for location sharing frequency (RQ2). South African respondents demonstrated higher preferences for transparency and control in ITS than Nordic participants. Lastly, we show that region and gender are relevant factors in shaping drivers' preferences for location privacy trade-offs (RQ3). Our analysis indicates that participants from South Africa were more likely to pay for PETs to enhance location privacy than participants from Nordic countries (RQ3). Additionally, the results showed a gender dependency in willingness to pay for pseudonyms, with females showing higher preferences for paying compared to males. There was also a significant difference in drivers' preferences for usability trade-off by gender, with males having higher preferences for usability than females, who rather favour privacy over usability.

5.1 The impact of region

Our results show that the region of drivers matters in the context of privacy attitudes and preferences. Below, we discuss our findings considering previous research and social aspects ingrained into the two regions.

5.1.1 Socioeconomic conditions and legal considerations. The results indicate that South Africans' risk perception is higher, and that the Nordic participants are more willing to take risks and have higher risk tolerance. Previous studies found the relationship between risk perception and wealth [40] in that individuals going through hardship, domestic wars, or poverty may be less risk-averse and vice versa. Thus, the difference in socioeconomic status might also explain the difference in willingness to take risks between the two regional groups. The more pronounced risk perceptions in South Africa may be explained by the high rates of crime in the country, including road and car crime [33, 52, 59, 77].

Similarly, South African drivers were more concerned about their location privacy in ITS than the Nordic group. Since the analysis showed that privacy concerns and risk perception impact privacy preferences, the results imply that South African preferences for future VANETs may be characterized by higher perceived risk and privacy concerns, which may impact trust in future ITS. Previous studies in other contexts have also shown South African consumers have privacy concerns regarding whether their personal information is used lawfully, for the agreed purposes, and that consent is not always obtained [17, 26].

On the other side, privacy concerns by users from Nordic EU countries were also shown to be in general low by previous Eurobarometer surveys [29, 30]. These survey revealed for instance that users from the Nordic EU countries have in common that they are usually less concerned about not having complete control over their data than users have on average in all EU countries. Swedes especially stick out as being on average least concerned among the EU country participants about having no or only partial control over their data.

The discrepancy in the privacy concerns shown in the two groups might also be due to the transparency and openness principles and regulations implemented in Nordic countries. Hence, people in the Nordic countries are already used to the idea that personal data about them kept by the governments can anyhow be easily obtained by others that exercise their respective transparency rights [46, 83].

In addition, we found regional discrepancies in preferences for transparency and control. The South African group was more eager than the Nordic participants to manage and control their location data used in ITS, which may be perceived as an essential means for avoiding privacy risks [57]. An explanation for this difference could be that Nordic countries are used to the rights of transparency and control guaranteed by a long tradition of openness and transparency laws as well as privacy laws and GDPR enforcement. According to the GDPR, the privacy principles of transparency and data subject rights for control should be guaranteed by design and default (in contrast to the POPI act that does not explicitly demand privacy by design and default). Moreover, non-compliance with the GDPR has since 2018 already resulted in a long record of high fines issued by data protection authorities of member states for organisations that have breached GDPR privacy principles, including the GDPR's transparency obligations[4]. Hence, people in the Nordic countries may have lower preferences and demands for transparency and control, as they may put higher trust in the implementation and enforcement of privacy rights and principles according to the GDPR and other laws. In contrast, the very short history of privacy regulations in South Africa may contribute to higher demands for privacy rights for transparency and control. The higher demand of South Africans for transparency and control can also be explained by previous findings that show that the South African society is characterised by low levels of trust in the institutions, and in their transparency and accountability [38, 53], which can be explained as a consequence of the former apartheid system [4].

The results also revealed that the Nordics exhibited lower preferences for cost trade-offs — paying for short-term pseudonyms to protect their privacy. While this might be apparent from the low privacy concerns they demonstrated concerning location data use in ITS, it should be interpreted differently for South African drivers. Their higher disposition towards paying for pseudonyms might be driven by their considerably greater privacy concerns and risk perceptions about their location data in ITS; hence, they may see value in paying for PETs to enhance data privacy. Moreover, among our participants, the majority were employed as well as educated. For this reason, and also as our study targeted participants who possess a driver's licence, it is likely that their socio-economic status was not extremely low; hence, such financial stability could affect their willingness to pay for privacy protection.

5.1.2 Regionally-ingrained sharing preferences. The two regional groups differed significantly in their preferences for sharing with different entities, especially with family and close friends. The collectivistic character of the South African society was confirmed

[4] See, e.g., GDPR Enforcement Tracker, https://www.enforcementtracker.com

by Triandis [82], and can relate to the African philosophy of *ubuntu*, implying that South Africans value the welfare of collective society, believe in the sense of belongingness and community [5]. Confirming the philosophy of *ubuntu* in South Africa, they seem to prioritize looking after their family and friends. Yet, another possible explanation for this difference might be the noticeably higher crime statistics in South Africa [52, 78] and related safety implications, which may imply that South Africans like to check on their family and close friends to ensure they are safe when they are out on the road.

We observed significant regional variations regarding preferences for sharing location data with entities such as insurance companies, emergency services, and police. South African participants had higher preferences for sharing location data with police, emergency services, and insurance companies than Nordic participants. The results that South African participants have higher preferences for sharing despite perceiving higher privacy concerns and risk may be seen as a contradiction to previous work showing that privacy concerns in other contexts reduce individuals' intention to disclose [47, 50]. However, an explanation could be that the sharing purposes we investigated in this work (e.g., personalized advertisement, combating car crime, or monitoring road safety), might have been perceived by South African respondents to a higher degree as benefits that are offered in case of sharing location data than by Nordic respondents, affecting their responses. Hence, the result can also be explained by and seen as in line with the theory of contextual integrity.

Particularly, enhanced preferences of the South African participants for sharing with these institutions may also be driven by the fact that compared to Nordics, they feel safe to a much lower extent [78]. Thus, South Africans may have high expectations in these institutions to ensure their safety and protect their personal information, as was observed in a comparison study between South Africa and the UK [18]. Another cross-country survey study between South Africa and Australia also reported South Africans' high expectations towards the government to protect their personal information in direct marketing [26].

5.1.3 Comparison with the previous interview studies. One objective of the present research was to validate the results of previous qualitative studies by Islami et al. [42, 43] [5]. Considering preferences for transparency and control, the present study found South African drivers exhibiting higher preferences for transparency and control than their Nordic counterparts. This result is somewhat different from the previous interview studies by Islami et al. [42, 43], which reported South African and Swedish drivers share similar demands for more control over location data in ITS, usable privacy notices, transparency and fine-grained settings.

Overall, the present findings are consistent with the previous results, indicating that South African participants have higher privacy concerns and risk perception than Nordic participants. The insights from the interview studies in Islami et al. [42, 43] identified South African drivers' concerns regarding location being tracked for criminal purposes, stalking and kidnapping. Conversely, Swedish drivers reported not being concerned about location data used in ITS.

Corroborating the qualitative study's results, the present results indicate that South African drivers have higher preferences to share location data with family and friends than Nordic participants. However, the results for sharing location data with other entities are not in line with past research [42, 43], which showed South African participants' higher reluctance to trust the government or police to access their location data than Swedish participants. This difference might be due to the different study designs: in the interviews, participants were asked about trust in external entities to protect their privacy, whereas, in the questionnaire, they were asked about their willingness to share location data with different entities for specific purposes (which would mostly benefit them).

While the present study reported preferences for cost trade-offs were higher among South Africans than among the Nordics, the past research showed the opposite [42, 43]. However, the Swedish participants' high preference to pay for short-term pseudonyms signed by a trusted third party to preserve their privacy was questioned to be influenced by the social desirability bias [9] or demand characteristics [54], which is more likely to happen in interviews than in surveys. On the other hand, South African participants voiced limited trust in PETs to protect their location privacy.

5.2 Discussion of findings other than regional differences

This section discusses our general findings other than regional differences and compare them with related work. Some of these general results resemble, or are similar to, past findings regarding location sharing by previous work that were also conducted for other applications or areas, which we discuss below. However, we still contribute with our work with new insights showing to what extent these related results from other areas also hold in the context of ITS and VANETs.

In the extensive review intended to explain the relationships between privacy attitudes and behaviour, Gerber et al. [35] showed that risk perception is associated with using location-based social networks. Similarly, in our findings, risk perceptions predict preferences to share location data; however, only when considering sharing with friends and family.

The finding that the entity that is receiving the information was an important factor in sharing decisions concurs with other works in the context of location sharing [12], dashcam video sharing [60] or in ubiquitous computing [51].

The fact that transparency influences location-sharing behaviour is found in other studies exploring users' perceptions of location privacy [6]. The major differences were that we explore the preferences of drivers for transparency and control in intelligent transportation systems and future VANETs from two different regions, while in Becker et al. [6], the authors survey participants on internet privacy concerns, cyber and physical risk taking, privacy victimisation, usage of location sharing apps and transport choices and segment them in clusters of risk perceptions and behaviour.

Our results also showed gender differences regarding risk perception and preference for usability-privacy trade-offs. Specifically, the analysis found females perceive higher risk and value privacy

[5] The methods used in the studies and different samples (past research included Swedish and South African participants) make the comparison somehow limited.

more important than usability for location data in ITS and vehicular communications. This could be explained by the fact that females are afraid of being stalked, as one study in the context of vehicular communication systems showed females rank safety higher than men [73]. The gender differences in preference for usability trade-off were shown in another study by Gardner et al. [32] in the context of location-based systems, which found that females were more willing to disclose their location in very coarse resolution (accuracy) in the cost of quality of service than men who were more in favour of compromising their privacy for getting the best service.

To some extent, our results indicate that people's concerns about privacy might have a negative effect on their information disclosure (i.e. if we define location sharing for specific purposes as disclosure). Such a finding adds to the body of knowledge around the privacy paradox—assumption that people tend to disclose personal information even though they are concerned about their privacy [35]. Our results oppose the privacy paradox and suggest that people might be making rational, in an economic sense, decisions, weighing the costs and benefits of information sharing, which is likely in the context of our research if the purpose of data sharing is considered. The predictive ability of privacy concerns correspond to privacy decision model derived from the past literature placing privacy concerns in a center [25], as well as research on this construct in other contexts. For instance, Zhang et al. [90] identified a negative relationship between privacy concerns and information disclosure in the context of health communities.

Still, some research indicates that privacy concerns are not the strongest predictor of information disclosure, and at times, design elements triggering heuristic-based decision-making might be sufficient to change the relationship between behaviour and information disclosure. For instance, Sundar et al. [79], through experimental design, showed that considering different visual cues and information disclosure context, only groups of participants presented with the authority cue (context of banking) and self-presentation cue (context of dating), privacy concerns were significant predictors of information disclosure. For instance, the control cue (control over publicly sharing information on social media) or transparency cue (context of privacy policies) privacy concerns were not significant predictors of information disclosure. The present research aimed to gather information about participants' preferences in order to design privacy profiles (see Section 5.3) and test them in the experimental research in future. Therefore, we expect that the strength of the effect that attitudinal factors (e.g., privacy concerns or risk perceptions) have on the sharing preferences might change in the future studies, similar to findings from Sundar et al. [79].

Despite some similarities that our findings share with previous studies, especially considering privacy concerns and risk perception, we must emphasize that when modelling location-sharing preferences, the effect size that these constructs have was smaller than the effect sizes of other variables—for instance, regional background, preferences for transparency and control, or preferences for sharing frequency were all more strongly associated with sharing preferences. This is particularly visible considering preferences for sharing location with the government, with other drivers and sharing for emergencies.

5.3 Outlook: Towards usable privacy and identity management for ITS

Previous research has shown that users are usually overwhelmed with the task of managing their privacy settings, that burdening users with this task of setting each individual permission is tedious and prone to errors, and that existing settings do often not accurately capture people's privacy preferences [71, 76].

In this section, we argue how our results can also help to address this problem and can provide valuable input for the design of usable privacy-enhancing identity management solutions for ITS and VANETs in compliance with legal privacy principles. Further elaborations of our suggested approaches towards a usable design are outlined below based on offering users suitable "bundles" of settings for easily getting started plus using machine learning (ML) to generate individualised recommendations for subsequently easily adapting settings, and will be part of our future research.

5.3.1 Predefined privacy profiles. For simplifying the management of privacy settings, privacy settings could be bundled into predefined privacy profiles of settings reflecting typical privacy preferences of parts of a population, which the users can then easily choose and possibly further adapt. These privacy profiles should be framed with a self-explanatory name and a short, high-level description, which can be expanded to show the detailed settings that are bundled.

Based on legal privacy requirements and the results of our study, the following types of privacy profiles could be offered for South African and Nordic drivers:

- **Privacy by Design and Default Profile for ITS.** First of all, to meet the privacy principles of data protection by design and default (Art. 25 GDPR) and data minimisation (Art. 5 GDPR, Chapter 3 POPI act), users should always start, per default, with the most privacy-friendly profile, which assures that by default only a minimal amount of personal data necessary for ITS are processed. It should particularly also enforce data minimisation for ITS with an appropriate level of pseudonymity offered by default (e.g. guaranteeing pseudonymity changes on a daily basis), taking into account their costs in relation to the given ITS context and related risks. Such a Privacy by Design and Default profile for ITS should always be activated as a default but can later be edited and adapted.
- **Regional Privacy Profiles.** Based on our results, regional privacy profile settings could be defined. Offering such privacy profiles that match the predominant privacy preferences in certain regions can help users to more easily manage their settings by simply selecting (and possibly further adapting) such a profile. For example, as a conclusion from our survey results, a regional "Preferred settings in South Africa" profile could be constructed and offered to drivers in South Africa that enable additional permissions for data sharing beyond the necessary permissions set in the "Privacy by Design and Default" profile for ITS. Such a profile could reflect the predominantly higher preferences of South African drivers for sharing data and could pre-set sharing with emergency services, and police for safety purposes or

in emergency situations (beyond life-threatening situations for which data sharing is always set by default). Similarly, it could include settings for easily enabling the sharing of location with family and close friends, who should however still be manually entered or confirmed by the user for retaining the final control.
It is however important that these more generous data-sharing settings are accompanied by usable transparency and control options for meeting both legal privacy requirements and, at the same time, the strong preferences by South Africans for transparency and control and for addressing their higher privacy concerns and perceived risks. Hence, user interfaces where the pre-defined profiles can be selected should also provide an appropriate description, e.g., in the case of "Preferred settings in South Africa" for informing about pre-set sharing settings for police and emergency services for emergency and safety purposes as well as with family and friends. When opening the settings, the purposes and context of the pre-set sharing options should be made transparent in further detail and control options for easily changing these settings should be made directly accessible.

- Moreover, our results suggest that **gender-specific profiles** or different gender-specific settings for regional profiles could be defined. For instance, since female participants prefer to trade usability for privacy, profiles for female drivers could pre-set location privacy features enforcing k-anonymity for them on the costs of lower usability. However, since our study was not designed with a main objective on gender-related aspects, our gender-related results and suggestions for gender-specific settings need to be taken with care and would need further follow-up studies including all gender representations to guarantee truly inclusive solutions.
- Pre-defined profiles or profile settings with stronger privacy/ pseudonymity levels that go beyond "appropriate" default pseudonymity (by implementing shorter time intervals for pseudonym changes, e.g. changes after one car ride, or after 10 minutes) can be offered for extra subscription costs/packages. Stronger pseudonymity settings that could be set for extra costs could especially be highlighted in the above-envisioned profiles for females, as our female participants showed a higher willingness to pay for better pseudonymity protection.

The development and design (particularly UI design) of the above-mentioned privacy profiles, particularly regional privacy profiles or gender-dependent profiles, must be well thought-through, considering the best practices, e.g., principles of Human Centered Design and/or Value Sensitive design, to ensure that interaction does not become burdensome. This opens an avenue for future research to investigate how interactions with such profiles should look and function to create useful and usable solutions.

5.3.2 Privacy preference prediction and recommendation. Machine-learning (ML)-based personalised privacy assistants, which have been developed in recent years for IoT applications (see, e.g. [11, 20, 69, 71]), can support users in easily making suitable adaptions to their privacy settings and chosen profiles. Our future research plans to further investigate how ML-based automated privacy assistants can observe the user's communication and behaviour for VANETs and/or other related IoT applications processing location data and then predict and recommend suitable individual privacy settings for VANETs for the user. Models predicting those factors that, according to our study results, deviated much among our participants (and thus seem to be highly different between users) could be trained, such as the frequency and granularity of data sharing or the entity with whom data is shared. For achieving both usable and privacy-enhancing identity management solutions, it is however important that the ML training is conducted in a privacy-friendly manner, e.g., locally on the user's device and under the user's control.

5.4 Limitations

Using hypothetical purposes to investigate drivers' preferences for sharing location data might be a design limitation of our study. Framing the purposes of sharing in ITS towards the positive (as potential benefits) might have affected participants' preferences, e.g. increasing the South Africans' willingness to share. Still, privacy policies texts are usually framed in terms of positive purposes for the data that should be collected and processed. Hence, our framing corresponds to policy framing that users are confronted with in realistic situations.

Another limitation is the lack of cultural representation of our sample. Hence, in this study, we can only discuss cross-regional (Nordics vs. South Africans) instead of cross-cultural differences. Future research should be conducted to compare the present results with other regions.

Because VANETs are the technology of the future, we introduced them together with existing ITS systems which the participants currently use, which might be limiting. Alternatively, we could have classified participants' privacy concerns using the privacy segmentations used before [28, 56, 87], clustering users in different privacy personas. However, such segmentations have been heavily criticised because they are poor predictors of context-specific behaviours [12, 89] (e.g., Westin/Harris Privacy Segmentation Model failed predicting location sharing decisions [12]) or that privacy categorization should not only consider a difference in degree but also in kind [48]. With privacy preferences being highly contextual and diverse and the poor correspondence between users' general privacy attitudes and their actual behaviours, we advocate that categorising users might not be possible.

A further constraint is a lack of a representative sample. Although it was not our main interest to investigate the effect of these demographics on privacy preferences for ITS, we cannot state that differences in privacy preferences across other demographic groups do not exist.

The main focus of the research is to assess the regional differences in the participants' preferences around sharing and trade-offs. When possible, we also looked at the effects that latent constructs, such as privacy concerns and risk perceptions, might have on participant preferences. However, for clarity, latent constructs were not included in the assessment of tradeoffs (RQ3) due to the methodological challenges (data analysis) their inclusion would instill.

We aimed to gain a deeper understanding of the privacy preferences of drivers for ITS. However, the number of predictive variables is limited and could account for other confounding factors, e.g., personality traits. On the other hand, incorporating personality traits in privacy-enhancing designs was shown to be problematic, e.g., personality traits-based personalization was proven unsuccessful [85]. Still, past research investigated other factors, such as driving style [65], or monetary rewards for sharing dashcam videos by drivers [60]. We plan to design experiments with visualisations of privacy profiles built upon our results, in which we plan to account for the previously studied confounding variables.

6 CONCLUSION

Our understanding of drivers' privacy preferences for ITS and future VANETs has been very limited, including the effects of latent factors and region on preferences for sharing in vehicular contexts. Hence, this article reports the results of an international comparison study based on a survey with 528 drivers from South Africa and the Nordics, whose analysis revealed a significant influence of region and latent constructs on preferences for ITS. The results particularly show that preferences for transparency and control are strongly related to willingness to share location data in ITS, this effect being more pronounced among the South African drivers than among the Nordics. Further, risk perceptions and privacy concerns are determinants of preferences for transparency and control. Tracing this relationship from the perspective of regional differences revealed individuals from South Africa with higher perceptions of risk and privacy concerns have higher demands for transparency and control in terms of location data being used in vehicular networks.

The article discusses also the implications of the results for designers and researchers of usable privacy for ITS and future VANETs. Correspondingly, the findings contribute to inferring viable predictors for the usable design of privacy-enhancing identity management systems for future VANETs that satisfy not only legal privacy principles but also the drivers' preferences and needs.

ACKNOWLEDGMENTS

This work has been funded by the Swedish Foundation for Strategic Research (SSF) SURPRISE Project. Simone Fischer-Hübner's contribution was also partially supported by the Wallenberg AI, Autonomous Systems and Software Program (WASP) funded by the Knut and Alice Wallenberg Foundation. We also thank Panos Papadimitratos for his very helpful technical insights about the location privacy trade-offs of PETs solutions for VANETs.

REFERENCES

[1] Sailesh Acharya and Michelle Mekker. 2022. Importance of the reputation of data manager in the acceptance of connected vehicles. *Communications in Transportation Research* 2 (2022), 100053.

[2] Sailesh Acharya and Michelle Mekker. 2022. Measuring data sharing intention and its association with the acceptance of connected vehicles. *Transportation research part F: traffic psychology and behaviour* 89 (2022), 423–436.

[3] Kalliopi Anastasopoulou, Emma Williams, Carolyn Whitnall, Theo Tryfonas, Elisabeth Oswald, Phil Morgan, Alexandra Voinescu, Robert Piechocki, and Andrea Tassi. 2018. Effects of privacy risk perception and cultural bias on intention of connected autonomous vehicle use. In *Proceedings of the 8th Workshop on Socio-Technical Aspects in Security and Trust*. Association for Computing Machinery, New York, NY, USA, 1–6. https://doi.org/10.1145/3361331.3361336

[4] Albert Arko-Cobbah. 2008. The right of access to information: Opportunities and challenges for civil society and good governance in South Africa. *IFLA journal* 34, 2 (2008), 180–191.

[5] Kwame Asamoah and Emmanuel Yeboah-Assiamah. 2019. "Ubuntu philosophy" for public leadership and governance praxis: Revisiting the ethos of Africa's collectivism. *Journal of Global Responsibility* 10, 4 (2019), 307–321.

[6] Ingolf Becker, Rebecca Posner, Tasmina Islam, Paul Ekblom, Hervé Borrion, Michael McGuire, and Shujun Li. 2021. Privacy in transport? Exploring perceptions of location privacy through user segmentation. *Proceedings of 54th Hawaii International Conference on System Sciences (HICSS 2021)* (2021), 5347–5356. https://doi.org/10.1109/TMC.2007.1062

[7] Giampaolo Bella, Pietro Biondi, and Giuseppe Tudisco. 2021. Car drivers' privacy concerns and trust perceptions. In *Trust, Privacy and Security in Digital Business: 18th International Conference, TrustBus 2021, Virtual Event, September 27–30, 2021, Proceedings 18*. Springer, 143–154.

[8] Michael Benisch, Patrick Gage Kelley, Norman Sadeh, and Lorrie Faith Cranor. 2011. Capturing location-privacy preferences: quantifying accuracy and user-burden tradeoffs. *Personal and Ubiquitous Computing* 15 (2011), 679–694.

[9] Nicole Bergen and Ronald Labonté. 2020. "Everything is perfect, and we have no problems": detecting and limiting social desirability bias in qualitative research. *Qualitative health research* 30, 5 (2020), 783–792.

[10] AJ Bernheim Brush, John Krumm, and James Scott. 2010. Exploring end user preferences for location obfuscation, location-based services, and the value of location. In *Proceedings of the 12th ACM international conference on Ubiquitous computing*. 95–104.

[11] Jessica Colnago, Yuanyuan Feng, Tharangini Palanivel, Sarah Pearman, Megan Ung, Alessandro Acquisti, Lorrie Faith Cranor, and Norman Sadeh. 2020. Informing the design of a personalized privacy assistant for the internet of things. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–13.

[12] Sunny Consolvo, Ian E Smith, Tara Matthews, Anthony LaMarca, Jason Tabert, and Pauline Powledge. 2005. Location disclosure to social relations: why, when, & what people want to share. In *Proceedings of the SIGCHI conference on Human factors in computing systems*. 81–90.

[13] Caitlin D Cottrill et al. 2015. Location privacy preferences: A survey-based analysis of consumer awareness, trade-off and decision-making. *Transportation Research Part C: Emerging Technologies* 56 (2015), 132–148.

[14] Mary J Culnan and Pamela K Armstrong. 1999. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization science* 10, 1 (1999), 104–115.

[15] Mitchell L Cunningham, Michael A Regan, Timothy Horberry, Kamal Weeratunga, and Vinayak Dixit. 2019. Public opinion about automated vehicles in Australia: Results from a large-scale national survey. *Transportation research part A: policy and practice* 129 (2019), 1–18.

[16] Dan Cvrcek, Marek Kumpost, Vashek Matyas, and George Danezis. 2006. A study on the value of location privacy. In *Proceedings of the 5th ACM workshop on Privacy in electronic society*. 109–118.

[17] Adele Da Veiga. 2018. An information privacy culture instrument to measure consumer privacy expectations and confidence. *Information & Computer Security* 26, 3 (2018), 338–364.

[18] Adéle Da Veiga and Jacques Ophoff. 2020. Concern for information privacy: a cross-nation study of the United Kingdom and South Africa. In *International Symposium on Human Aspects of Information Security and Assurance*. Springer, 16–29.

[19] George Danezis, Stephen Lewis, and Ross J Anderson. 2005. How much is location privacy worth?. In *WEIS*, Vol. 5. 56.

[20] Anupam Das, Martin Degeling, Daniel Smullen, and Norman Sadeh. 2018. Personalized privacy assistants for the internet of things: Providing users with notice and choice. *IEEE Pervasive Computing* 17, 3 (2018), 35–46.

[21] Patrick Dattalo. 2013. *Analysis of multiple dependent variables*. Oxford University Press, USA.

[22] Manfred FR Kets De Vries. 2006. *The leadership mystique: Leading behavior in the human enterprise*. Pearson Education.

[23] Sebastian Derikx, Mark De Reuver, and Maarten Kroesen. 2016. Can privacy concerns for insurance of connected cars be compensated? *Electronic markets* 26 (2016), 73–81.

[24] Rinku Dewri and Ramakrisha Thurimella. 2014. Exploiting Service Similarity for Privacy in Location-Based Search Queries. *IEEE Transactions on Parallel and Distributed Systems* 25, 2 (2014), 374–383. https://doi.org/10.1109/TPDS.2013.34

[25] Tamara Dinev, Allen R McConnell, and H Jeff Smith. 2015. Research commentary—informing privacy research through information systems, psychology, and behavioral economics: thinking outside the "APCO" box. *Information Systems Research* 26, 4 (2015), 639–655.

[26] Sara Dolnicar and Yolanda Jordaan. 2007. A market-oriented approach to responsibly managing information privacy concerns in direct marketing. *Journal of advertising* 36, 2 (2007), 123–149.

[27] Matt Duckham and Lars Kulik. 2006. Location privacy and location-aware computing. In *Dynamic and mobile GIS*. CRC press, 63–80.

[28] Janna Lynn Dupree, Richard Devries, Daniel M Berry, and Edward Lank. 2016. Privacy personas: Clustering users via attitudes and behaviors toward security practices. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. 5228–5239.

[29] EU Commission. 2015. *Special Eurobarometer 431 – Data Protection*. Technical Report.

[30] EU Commission. 2019. *Special Eurobarometer 487a – The General Data Protection Regulation*. Technical Report.

[31] EF Education First. 2023. EF English Proficiency Index. https://www.ef.com/wwen/epi/

[32] Zoe Gardner, Didier Leibovici, Anahid Basiri, and Giles Foody. 2017. Trading-off location accuracy and service quality: Privacy concerns and user profiles. In *2017 International Conference on Localization and GNSS (ICL-GNSS)*. IEEE, 1–5.

[33] Rufaro Garidzirai and Rufaro Emily Chikuruwo. 2020. An economic analysis of the social grant policy in South Africa. *Journal of Advanced Research in Law and Economics* 11, 2 (48) (2020), 362–369.

[34] Bugra Gedik and Ling Liu. 2008. Protecting Location Privacy with Personalized k-Anonymity: Architecture and Algorithms. *IEEE Transactions on Mobile Computing* 7, 1 (2008), 1–18. https://doi.org/10.1109/TMC.2007.1062

[35] Nina Gerber, Paul Gerber, and Melanie Volkamer. 2018. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & security* 77 (2018), 226–261.

[36] Joseph A Gliem and Rosemary R Gliem. 2003. Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for Likert-type scales. Midwest Research-to-Practice Conference in Adult, Continuing, and Community Education.

[37] Norbert Götz. 2015. The concept of openness: promise and paradox. In *The Paradox of Openness*. Brill, 10–26.

[38] Amanda Gouws and Collette Schulz-Herzenberg. 2016. What's Trust Got to do with it? Measuring Levels of Political Trust in South Africa 20 Years after Democratic Transition. *Politikon* 43, 1 (2016), 7–29.

[39] Marco Gruteser and Dirk Grunwald. 2003. Anonymous usage of location-based services through spatial and temporal cloaking. In *Proceedings of the 1st international conference on Mobile systems, applications and services*. 31–42.

[40] Luigi Guiso and Monica Paiella. 2008. Risk aversion, wealth, and background risk. *Journal of the European Economic association* 6, 6 (2008), 1109–1150.

[41] Vipin Gupta, Paul J Hanges, and Peter Dorfman. 2002. Cultural clusters: Methodology and findings. *Journal of world business* 37, 1 (2002), 11–15.

[42] Lejla Islami, Simone Fischer-Hübner, Eunice Naa Korkoi Hammond, and Jan Eloff. 2021. Analysing Drivers' Preferences for Privacy Enhancing Car-to-Car Communication Systems: A Study from South-Africa. In *Privacy and Identity Management: 15th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2. 2 International Summer School, Maribor, Slovenia, September 21–23, 2020, Revised Selected Papers 15*. Springer, 115–133.

[43] Lejla Islami, Simone Fischer-Hübner, and Panos Papadimitratos. 2022. Capturing drivers' privacy preferences for intelligent transportation systems: An intercultural perspective. *Computers & Security* 123 (2022), 102913.

[44] Hongyu Jin and Panos Papadimitratos. 2019. Resilient privacy protection for location-based services through decentralization. *ACM Transactions on Privacy and Security (TOPS)* 22, 4 (2019), 1–36.

[45] Leslie K John, Alessandro Acquisti, and George Loewenstein. 2011. Strangers on a plane: Context-dependent willingness to divulge sensitive information. *Journal of consumer research* 37, 5 (2011), 858–873.

[46] Oluf Jørgensen. 2014. *Access to Information in the Nordic Countries. A comparison of the laws of Sweden, Finland, Denmark, Norway and Iceland and international rules*. Nordic Council of Ministers, Nordicom.

[47] Flavius Kehr, Tobias Kowatsch, Daniel Wentzel, and Elgar Fleisch. 2015. Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal* 25, 6 (2015), 607–635.

[48] Bart P Knijnenburg, Alfred Kobsa, and Hongxia Jin. 2013. Dimensionality of information disclosure behavior. *International Journal of Human-Computer Studies* 71, 12 (2013), 1144–1162.

[49] Nils Koester, Patrick Cichy, David Antons, and Torsten-Oliver Salge. 2021. Privacy Risk Perceptions in the Connected Car Context. (2021).

[50] Hanna Krasnova, Sarah Spiekermann, Ksenia Koroleva, and Thomas Hildebrand. 2010. Online social networks: Why we disclose. *Journal of information technology* 25, 2 (2010), 109–125.

[51] Scott Lederer, Jennifer Mankoff, and Anind K Dey. 2003. Who wants to know what when? privacy preference determinants in ubiquitous computing. In *CHI'03 extended abstracts on Human factors in computing systems*. 724–725.

[52] Macrotrends. 2023. Crime Rate & Statistics by Country. https://www.macrotrends.net/countries/ranking/crime-rate-statistics

[53] DL Marais, M Quayle, and JK Burns. 2017. The role of access to information in enabling transparency and public participation in governance-a case study of access to policy consultation records in South Africa. *African Journal of Public Affairs* 9, 6 (2017), 36–49.

[54] Jim McCambridge, Marijn De Bruin, and John Witton. 2012. The effects of demand characteristics on research participant behaviours in non-laboratory settings: a systematic review. *PloS one* 7, 6 (2012), e39116.

[55] Imran Memon, Qasim Ali Arain, Muhammad Hammad Memon, Farman Ali Mangi, and Rizwan Akhtar. 2017. Search me if you can: Multiple mix zones with location privacy protection for mapping services. *International Journal of Communication Systems* 30, 16 (2017), e3312.

[56] Anthony Morton and M Angela Sasse. 2014. Desperately seeking assurances: Segmenting users by their information-seeking preferences. In *2014 Twelfth Annual International Conference on Privacy, Security and Trust*. IEEE, 102–111.

[57] Patrick Murmann, Matthias Beckerle, Simone Fischer-Hübner, and Delphine Reinhardt. 2021. Reconciling the what, when and how of privacy notifications in fitness tracking scenarios. *Pervasive and Mobile Computing* 77 (2021), 101480. https://doi.org/10.1016/j.pmcj.2021.101480

[58] Helen Nissenbaum. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press, Redwood City. https://doi.org/doi:10.1515/9780804772891

[59] Numbeo. 2021. Crime Index by Country 2023 Mid-Year. https://www.numbeo.com/crime/rankings_by_country.jsp. [Online; accessed 24-July-2023].

[60] Sangkeun Park, Joohyun Kim, Rabeb Mizouni, and Uichin Lee. 2016. Motives and concerns of dashcam video sharing. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. 4758–4769.

[61] Eyal Peer, Laura Brandimarte, Sonam Samat, and Alessandro Acquisti. 2017. Beyond the Turk: Alternative platforms for crowdsourcing behavioral research. *Journal of Experimental Social Psychology* 70 (2017), 153–163.

[62] Andreas Pfitzmann and Marit Hansen. 2010. A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management.

[63] Maija Poikela and Eran Toch. 2017. Understanding the valuation of location privacy: a crowdsourcing-based approach. (2017).

[64] Sören Preibusch. 2013. Guide to measuring privacy concern: Review of survey and observational instruments. *International journal of human-computer studies* 71, 12 (2013), 1133–1143.

[65] Carlo Pugnetti and Sandra Elmer. 2020. Self-assessment of driving style and the willingness to share personal information. *Journal of Risk and Financial Management* 13, 3 (2020), 53.

[66] Thomas G Reio Jr and Brad Shuck. 2015. Exploratory factor analysis: implications for theory, research, and practice. *Advances in developing human resources* 17, 1 (2015), 12–25.

[67] Alvin C Rencher and G Bruce Schaalje. 2008. *Linear models in statistics*. John Wiley & Sons.

[68] Stephen Cory Robinson. 2020. Trust, transparency, and openness: How inclusion of cultural values shapes Nordic national public policy strategies for artificial intelligence (AI). *Technology in Society* 63 (2020), 101421.

[69] Norman Sadeh, Jason Hong, Lorrie Cranor, Ian Fette, Patrick Kelley, Madhu Prabaker, and Jinghai Rao. 2009. Understanding and capturing people's privacy policies in a mobile social networking application. *Personal and ubiquitous computing* 13 (2009), 401–412.

[70] Pierangela Samarati and Latanya Sweeney. 1998. Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression. (1998).

[71] Odnan Ref Sanchez, Ilaria Torre, Yangyang He, and Bart P Knijnenburg. 2020. A recommendation approach for user privacy preferences in the fitness domain. *User Modeling and User-Adapted Interaction* 30 (2020), 513–565.

[72] Teresa Schmidt, Ralf Philipsen, Philipp Themann, and Martina Ziefle. 2016. Public perception of V2x-technology-evaluation of general advantages, disadvantages and reasons for data sharing with connected vehicles. In *2016 IEEE Intelligent Vehicles Symposium (IV)*. IEEE, 1344–1349.

[73] Teresa Schmidt, Ralf Philipsen, and Martina Ziefle. 2016. User diverse privacy requirements for V2X-technology-quantitative research on context-based privacy aspects. In *International Conference on Vehicle Technology and Intelligent Transport Systems*, Vol. 2. SCITEPRESS, 60–67.

[74] Brandon Schoettle and Michael Sivak. 2014. A survey of public opinion about connected vehicles in the US, the UK, and Australia. In *2014 International Conference on Connected Vehicles and Expo (ICCVE)*. IEEE, 687–692.

[75] Xan Smiley. 1999. Survey: the nordic countries: happy family. *The Economist* 350, 8103 (1999), N3ąN6.

[76] Daniel Smullen, Yuanyuan Feng, Shikun Zhang, and Norman M Sadeh. 2020. The Best of Both Worlds: Mitigating Trade-offs Between Accuracy and User Burden in Capturing Mobile App Privacy Preferences. *Proc. Priv. Enhancing Technol.* 2020, 1 (2020), 195–215.

[77] Statistics South Africa stats sa. 2023. Census 2022 – Crime in South Africa up in 202223. https://www.statssa.gov.za/?p=16562

[78] Stats SA – Statistics South Africa. 2022. STATISTICAL RELEASE P0341 Victims of Crime.

[79] S. Shyam Sundar, Jinyoung Kim, Mary Beth Rosson, and Maria D. Molina. 2020. Online Privacy Heuristics that Predict Information Disclosure. *Conference on Human Factors in Computing Systems - Proceedings* (4 2020). https://doi.org/10.1145/3313831.3376854

[80] Barbara G. Tabachnick and Linda S. Fidell. 2019. *Using Multivariate Statistics 5.* 980 pages.
[81] Eran Toch, Justin Cranshaw, Paul Hankes Drielsma, Janice Y Tsai, Patrick Gage Kelley, James Springfield, Lorrie Cranor, Jason Hong, and Norman Sadeh. 2010. Empirical models of privacy in location sharing. In *Proceedings of the 12th ACM international conference on Ubiquitous computing.* 129–138.
[82] Harry C Triandis. 1989. The self and social behavior in differing cultural contexts. *Psychological review* 96, 3 (1989), 506.
[83] Juho Vesa. 2015. Nordic openness in practice. *Nordicom Review* 36, 2 (2015), 129–142.
[84] Jonas Walter and Bettina Abendroth. 2020. On the role of informational privacy in connected vehicles: A privacy-aware acceptance modelling approach for connected vehicular services. *Telematics and Informatics* 49 (2020), 101361.
[85] Logan Warberg, Alessandro Acquisti, and Douglas Sicker. 2019. Can privacy nudges be tailored to individuals' decision making and personality traits? *Proceedings of the ACM Conference on Computer and Communications Security* (2019), 175–197. Issue Study 1. https://doi.org/10.1145/3338498.3358656
[86] Alan F Westin. 1968. Privacy and freedom. *Washington and Lee Law Review* 25, 1 (1968), 166.
[87] Alan F Westin. 2003. Social and political dimensions of privacy. *Journal of social issues* 59, 2 (2003), 431–453.
[88] RE Woliver and RB Cattell. 1981. Reoccurring national patterns from 30 years of multivariate cross-cultural studies. *International Journal of Psychology* 16, 1-4 (1981), 171–198.
[89] Allison Woodruff, Vasyl Pihur, Sunny Consolvo, Laura Brandimarte, and Alessandro Acquisti. 2014. Would a Privacy Fundamentalist Sell Their DNA for $1000...If Nothing Bad Happened as a Result? The Westin Categories, Behavioral Intentions, and Consequences. In *10th Symposium On Usable Privacy and Security (SOUPS 2014).* USENIX Association, Menlo Park, CA, 1–18. https://www.usenix.org/conference/soups2014/proceedings/presentation/woodruff
[90] Tingru Zhang, Da Tao, Xingda Qu, Xiaoyan Zhang, Rui Lin, and Wei Zhang. 2019. The roles of initial trust and perceived risk in public's acceptance of automated vehicles. *Transportation research part C: emerging technologies* 98 (2019), 207–220.

A SURVEY INSTRUMENT

A.1 Part I

Intelligent Transportation System (ITS) is the deployment of digital technologies and systems in vehicles (e.g., cars or trucks) and road infrastructure with the aim of improving road safety, efficiency and mobility. Imagine current systems like Waze or Garmin, that include services for car navigation, parking assistance, etc. The future ITS will exploit the communication of vehicles with each-other (for example, a vehicle can warn other vehicles nearby when it performs an emergency braking maneuver) and with the road infrastructure (for example, to guide drivers to empty parking slots) to exchange information. This will give drivers the ability to manage the driving more safely and efficiently (for example, about speed changing). The picture below illustrates the ITS model that focuses on capturing information generated by vehicles (such as location, sensor data) and road infrastructure. The information is then processed and delivered back to drivers to support a number of safety applications, including collision warnings, maintaining a safe speed and distance, lane keeping and change assistance, etc. This model is further enhanced by vehicles sharing information with each other and with the infrastructure.

A.2 Part II

In this section you will be asked about your general attitudes regarding Intelligent Transportation Systems. Please answer honestly based on how you really are, not how you would like to be.

Imagine you are a driver in a car using an Intelligent Transportation System which captures your location data (data which indicate the geographic position and whereabouts of a device or a car, i.e, GPS coordinates, GPS traces, mileage, routes taken, etc.). Please rate the extent to which you agree with the following:

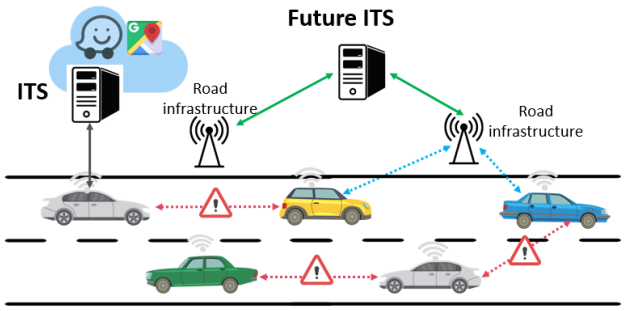

Figure 3: Overview of ITS

- I am concerned that the location information I disclosed to the intelligent transportation system could be misused.
- I am concerned about providing location information to the intelligent transportation system, because of what others might do with it.
- I am concerned about providing location information to the intelligent transportation system, because it could be used in a way I did not foresee.
- I am worried that if I use intelligent transportation systems, I might get tracked by the government.
- Using intelligent transportation systems involves the risk of getting stalked.
- I am worried that using intelligent transportation systems would lead to my home location being revealed.
- I am worried that using intelligent transportation systems involves the risk of becoming a victim of identity theft.
- I am worried that if I use intelligent transportation systems, strangers might know too much about my activities.
- Using intelligent transportation systems poses a threat to my personal safety.

In this section you will be asked about your preferences regarding Intelligent Transportation Systems. Please answer honestly based on how you really are, not how you would like to be.

Imagine you are a driver in a car using an Intelligent Transportation System which captures your location data. Please rate the extent to which you agree with the following:

- I would prefer to dedicate my time to managing the data (to control who can access it, with whom it is shared) collected about myself by the intelligent transportation system.
- I would prefer to make a cognitive effort to manage the data (to control who can access it, with whom it is shared) collected about myself by the intelligent transportation system.
- I would prefer easy-to-read policy information from the intelligent transportation system regarding the data collected about me and how and for what purpose my data will be processed.

- It is important to me that I am aware of any processing and profiling the intelligent transportation system has done about me.

A.3 Part III

In this section you will be asked about your preferences regarding Intelligent Transportation Systems. Please answer honestly based on how you really are, not how you would like to be.

Imagine you are a driver in a car using an Intelligent Transportation System which captures your location data. Please rate the extent to which you agree with the following:

- Considering the purposes of sharing my data, I am comfortable sharing my location data with my close family ...
  - for emergency
  - to check on them (ensure that they are safe and healthy)
  - for coordination of family activities (to ask whether they are coming for lunch, etc.)
  - to maintain a relationship
- Considering the purposes of sharing my data, I am comfortable sharing my location data with close friends ...
  - for emergency
  - to check on them (ensure that they are safe and healthy)
  - for coordination of family activities (to ask whether they are coming for lunch, etc.)
  - to maintain a relationship
- Considering the purposes of sharing my data, I am comfortable sharing my location data with other car drivers ...
  - for my own gain (route planning, receiving warnings about traffic situations, etc.)
  - for providing assistance for urgent health situations
  - for providing assistance for urgent mechanical situations (change of tyre, etc.)
  - for traffic safety (to report hazards, collisions, road conditions, etc.)
  - for interpersonal communication (sharing tips about social activities, for example, good restaurants on the way, tourist attractions)
- Considering the purposes of sharing my data, I am comfortable sharing my location data with the police ...
  - for traffic planning (rerouting traffic in case of traffic jams / accidents))
  - for monitoring road safety
  - for combating car crime
  - for car crash investigation
- Considering the purposes of sharing my data, I am comfortable sharing my location data with the government of the country I live in ...
  - for long-term traffic management
  - for environmental sustainability (pollution abatement)
  - for designing better infrastructure
  - for improving public services (monitor cross-border mobility, map tourist flows, etc.)
  - for research purposes (to establish open repositories for location data, partner with research institutions for data sharing and analysis)
- Considering the purposes of sharing my data, I am comfortable sharing my location data with insurance companies ...
  - for usage-based insurance policies (insurance fee is adopted based on your actual car use, measured mileage, driving behavior, etc.)
  - for car insurance liability (protects other drivers in accidents you are at fault by covering medical bills and property damage)
  - for better management of risk (the assessment of the likelihood and impact of events that may occur)
  - for personalized advertisement (relevant offerings, insurance premiums, etc.)
- Considering the purposes of sharing my data, I am comfortable sharing my location data with emergency services ...
  - for emergency purposes in case of accidents
  - for emergency mechanical situations (flat tire, battery not working, locked out of your car, brakes do not work)
  - for improvement of emergency strategies
  - for emergency data analytics
  - for growth of voluntary-based emergency services network
- Considering the frequency and type of location data, I am comfortable sharing my location data ...
  - when driving
  - only when driving to generic locations (work, home, university, etc.)
  - only when driving to unlabelled locations (undefined GPS coordinates, for example 39°36.06'N, GPS traces, Wi-Fi traces, etc.)

A.4 Part IV

In this section you will be asked about your preferences about usability trade-off that need to be made for future Intelligent Transportation Systems.

Imagine yourself in the scenario below and please indicate your actual preferences and not how you want to behave.

Your current Intelligent Transportation System can identify you and see your precise location. There is the option to design different, more-privacy-friendly systems, that gets less detailed location data from you and hence, knows less about you and cannot, or at least not easily identify you.

This is demonstrated by the scenario of a navigation application searching for available parking spots in your nearby, for which you could get two different navigation maps.

In the first one (Figure 2 A) you would receive a map with parking places in the specific street you are interested in, but as you are at that moment the only driver in the area, you can be easily identified.

In the second map (Figure 2 B), you receive a map with parking places for a larger region and, as at the specific time when the location data is collected, there are at least k other drivers in that area. Consequently, that location cannot uniquely identify you. This is because all drivers share their location at that time. However, this system (Figure 2 B) offers you a lower level of usability as you

would have to zoom in on the map and find your way to the parking spot on the preferred street.

Would you be willing to share your exact location for usability (Figure 2 A) in this case?

- Yes, I prefer the best usability possible because I do not have privacy concerns
- Yes, I prefer the best usability possible although I still have some privacy concerns
- I do not care about usability
- No, I want to protect my location data

In this section you will be asked about your preferences about cost trade-off that need to be made for future Intelligent Transportation Systems.

Imagine yourself in the scenario below and please indicate your actual preferences and not how you want to behave.

The current Intelligent Transportation System you are using can identify you and see your exact location. In order not to be uniquely known by the real name (identity), future systems may instead use aliases or pseudonyms for you, which are identifiers other than real names. However, if you always use the same pseudonym, different usages of the same pseudonym can be linked to each other and could finally also be related to you (e.g. if you park your car regularly in front of your house, a pseudonym that is frequently also used for your home address, is likely relating to you). Therefore, it is better to change the pseudonym often, but that costs more money as you have to pay for obtaining more pseudonyms from an issuing party. This system that uses pseudonyms that you frequently change (short-term pseudonyms) to make it harder for others to identify you is illustrated in the image below.

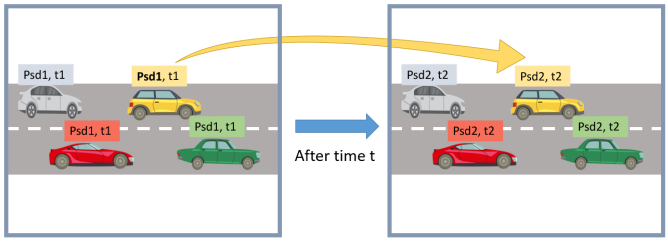

Figure 4: Cost trade-off

Would you be willing to pay more in order to hide your location data?

- Yes
- No

As described in the scenario above, the more you pay the more frequently would the pseudonyms be exchanged, hence, the better the privacy.

Please indicate how much you would like to pay to increase your privacy.

- nothing – no privacy protection based on pseudonyms
- 10 SEK per year – basic privacy protection
- 100 SEK per year – advanced privacy protection
- 500 SEK per year – premium privacy protection

A.5 Part V

Thank you for sharing your attitudes and preferences for location data.

This is the last part of the study. In this section you will be asked about your demographic characteristics.

- What is your country of residence?
  - South Africa
  - Sweden
  - Norway
  - Denmark
  - Iceland
  - Finland
- What is your age group?
  - 18-24
  - 25-34
  - 35-44
  - 45-54
  - 55-64
  - 65+
  - Prefer not to say
- How would you describe your gender?
  - Male
  - Female
  - Other
  - Prefer not to say
- What is the highest level of education you have completed?
  - Less than high school
  - High school or Professional qualification
  - University degree
  - Master's degree
  - Doctoral degree
  - Prefer not to say
- What is your current status of employment?
  - Employed
  - Unemployed
  - Student
  - Retired
  - Prefer not to say
- Do you use any intelligent transportation system or navigation application for the car?
  - Yes
  - No

  If yes, which one?

B EXPLORATORY FACTOR ANALYSIS

Table 6: Privacy preferences scale. Results of Exploratory Factor Analysis.

Factor	Items	Factor loading
Sharing with government, α = .92	I am comfortable sharing my location data with the government of the country I live in for environmental sustainability	.703
	I am comfortable sharing my location data with the government of the country I live in for long-term traffic management	.665
	I am comfortable sharing my location data with the government of the country I live in for designing better infrastructure	.631
	I am comfortable sharing my location data with the government of the country I live in for research purposes	.621
	I am comfortable sharing my location data with the government of the country I live in for improving public services	.525
Sharing with family and close friends, α = .88	I am comfortable sharing my location data with close friends to maintain a relationship	.853
	I am comfortable sharing my location data with my close family to maintain a relationship	.813
	I am comfortable sharing my location data with close friends for coordination of social activities	.775
	I am comfortable sharing my location data with my close family for coordination of family activities	.739
	I am comfortable sharing my location data with close friends to check on them	.521
	I am comfortable sharing my location data with my close family to check on them	.461
Sharing for emergency purposes, α = .66	I am comfortable sharing my location data with my close family for emergency	.696
	I am comfortable sharing my location data with close friends for emergency	.510
	I am comfortable sharing my location data with emergency services for emergency purposes in case of accidents	.483
Sharing with insurance companies, α = .89	I am comfortable sharing my location data with insurance companies for car insurance liability	.923
	I am comfortable sharing my location data with insurance companies for usage-based insurance policies	.897
	I am comfortable sharing my location data with insurance companies for better management of risk	.830
	I am comfortable sharing my location data with insurance companies for personalized advertisement	.463
Sharing with emergency services, α = .88	I am comfortable sharing my location data with emergency services for emergency data analytics	.910
	I am comfortable sharing my location data with emergency services for improvement of emergency strategies	.795
	I am comfortable sharing my location data with emergency services for growth of voluntary-based emergency services network	.694
	I am comfortable sharing my location data with emergency services for emergency mechanical situations	.455
Sharing with police, α = .92	I am comfortable sharing my location data with the police for combating car crime	.840
	I am comfortable sharing my location data with the police for monitoring road safety	.757
	I am comfortable sharing my location data with the police for car crash investigation	.675
	I am comfortable sharing my location data with the police for traffic planning	.656
Sharing with other drivers, α = .84	I am comfortable sharing my location data with other car drivers for providing assistance for urgent health situations	.801
	I am comfortable sharing my location data with other car drivers for providing assistance for urgent mechanical situations	.798
	I am comfortable sharing my location data with other car drivers for traffic safety	.722
	I am comfortable sharing my location data with other car drivers for my own gain	.474