Analysing Drivers' Preferences for Privacy Enhancing Car-to-Car Communication Systems

Lejla Islami, Simone Fischer-Hübner, Eunice Hammond, Jan Eloff

Analysing drivers' preferences for privacy enhancing car-to-car communication systems

Lejla Islami[1], Simone Fischer Hübner[1], Eunice Naa Korkoi Hammond[2] and Jan Eloff[2]

[1] Karlstad University, Karlstad, Sweden
[2] University of Pretoria, South Africa
lejla.islami@kau.se

Abstract. While privacy-enhancing solutions for car-to-car communication are increasingly researched, end user aspects of such solutions have not been in the focus. In this paper, we present a qualitative study with 16 car drivers in South Africa for analysing their privacy perceptions and preferences for control and privacy trade-offs, which will allow to derive end user requirements for privacy and identity management for vehicular communication systems. Our results show that while the South African participants are willing to share their location data with family and close friends, they often lack trust in external entities. They perceive safety implications from criminals and hackers and therefore dispel constant location tracking. Usability, privacy and safety are top priorities, with differing privacy – usability trade-offs for different users. The results show that participants demand more control over their privacy and seek usable privacy notices, transparency and fine-grained controls.

Keywords: Vehicular communication · privacy-enhancing technologies (PETs) · privacy perception · privacy preferences · usable privacy and identity management

1 Introduction

Future vehicular communication systems can bring many benefits for society, enhancing transportation safety, efficiency and convenience for drivers [17]. However, they pose privacy challenges at the same time. Continuous collection of users' location data enables to profile the drivers' locations and to derive sensitive information, e.g. about their activities or social contacts. Driving data is expected to be a 1.2 trillion euro market by 2030 [13], and thus there is an interest to use these data for different purposes. At the same time, many users may want to benefit from the wide range of applications, from infotainment services, navigation services, collision avoidance alerts and traffic condition updates, as long as their privacy is protected. The deployment of the continuous advances in vehicular ad hoc networks (VANETs) may only become a reality after the security and privacy of users are safeguarded [21]. There have been an extensive research on enabling fundamental security and privacy building blocks for the

introduction of such systems in the future (e.g., [16, 17]). Focusing on achieving anonymity and unlinkability in car-to-car communication systems, most of the proposals are pseudonym-based solutions [23]. Despite the importance of the development of privacy-enhancing solutions for vehicle communication, we know little about users' perceptions about the potential trade-offs of these solutions and their preferences and requirements in regard to privacy trade-off settings. We argue that it is essential to understand users' perception and preferences and to elicit their privacy requirements for implementing usable privacy and identity management solutions for VANETs, which are based on usable configuration options offering suitable selectable privacy settings that similar-minded users share.

Therefore, within the scope of our study we are motivated to address the following research questions:

- **RQ1:** *What privacy perceptions and preferences for data sharing and control do South African drivers have for car-to-car communication systems?*
- **RQ2:** *What are their preferences concerning trade-offs of location privacy vs. costs, safety and utility and usability?*

As privacy is a cultural construct [18], user requirements and preferences may differ culturally. Within the scope of the SSF project SURPRISE and a SASUF (South Africa – Sweden University Forum) – funded project, we have the ultimate goal to conduct an intercultural comparison study by researching these questions in Sweden and South Africa. As a first step in this direction, we conducted 16 semi-structured interviews with car drivers in South Africa. This paper reports about the findings of this first study, on which we will base our future research on usable privacy and identity management for VANETs.

The remainder of this paper is structured as follows: The following section 2 presents as Background the current role of privacy in South Africa and briefly explains how far privacy trade-offs need to be made for privacy-enhancing VANETs. Section 3 is then presenting the methodology that we took for conducting and evaluating the interviews. The results of the interviews are then presented in section 4 followed by a discussion in section 5. Section 6 is then discussing related work before final conclusions and an outlook are provided in section 7.

2 Background

This section first explains the role of privacy in South Africa, and then the privacy trade-offs to be made for privacy-enhancing VANETs.

2.1 Privacy in South Africa

From social gatherings to backyard entertainment, South Africans are inevitably one of the most sociable groups of people around the world [30]. However, this

may come as a contrast to the amount of value nationals and residents place on their security and safety on day to day activities and living. With the ever increasing crime rate in the country [11], many South Africans choose to invest in putting a guard on their surroundings. This has not only taken place in their physical environments, but also on various online communication streams and other interactions.

Views on privacy may be largely impacted through knowledge of the European Union's (EU) General Data Protection Regulation (GDPR) [10], yet South Africa's version of the privacy protection act, the Protection of Personal Information (POPI) Act [22], is one that may also ensure that privacy is protected and preserved. Signed into a law in late 2013, this act is targeted at the protection of personal information of individuals, with highlights on the confidentiality and integrity of this personal digital information, amongst others [8].

Privacy preferences by South Africans are more generally by preference, and one would hope that by an assurance of the safety of data and information, the average South African will likely have their hearts at rest, that is, by their data being protected (i.e. private), they will be safe. Nonetheless, this does not seem to be the case, as research shows that the gap between the expectations that people have about their privacy protection and whether or not these expectations are being met, is quite high [7]. A recent study [6] revealed that 91.8% of the participants had these high expectations concerning their privacy yet remained concerned when they have to share this information, especially online [6].

With this, it appears there is a clear contradiction as to what is stated in the POPI Act versus what many nationals actually experience, and whether this is intentional or not, this raises doubts in many hearts and minds and establishes the "concern for information privacy", as to whether or not their safety is actually guaranteed, as a result of these privacy expectations [6].

2.2 Privacy Trade-offs

Through an interview with experts researching privacy-enhancing VANETs from the SURPRISE project, we identified privacy trade-offs that may have to be made for privacy-enhancing solutions with costs, utility, usability and safety, which are also partly discussed in [23].

We are focusing on privacy-enhancing solutions based on short-lived pseudonyms and k-anonymity as the most commonly used, especially by our partners of the SURPRISE project(e.g., [16, 17]). For such solutions the privacy trade-offs can be summarised as follows: the shorter the time periods with that pseudonyms are exchanged, the lower the degree of linkability and thus the higher privacy protection. However, exchanging pseudonyms frequently implies higher costs for obtaining more signed pseudonyms from the issuing party (trade-offs with costs). Moreover, traffic collisions may be more difficult to predict the shorter the time periods are (trade-offs with traffic safety). On the other side, the more frequent traffic information is submitted, the higher the quality of traffic information.

However, if pseudonyms are often reused in a period of time, the degree of linkability raises (trade-offs with quality/utility).

Another privacy-enhancing technique is using obfuscation by generalizing the spatiotemporal information related to the drivers' location information, such that the location of a driver cannot be distinguished from that of at least k-1 other drivers, thus achieving k-anonymity [28]. For PET solutions with k-anonymous location privacy, privacy trade-offs with utility, and thus with usability, arise as well, as we will illustrate below.

3 Methodology

We conducted 16 semi-structured interviews with car drivers in South Africa to analyse what privacy perceptions and preferences drivers have for car-to-car communication systems and to find out how would they trade-privacy off with other goals such as costs, usability, data quality, safety. The study was approved by Research Ethics Board at University of Pretoria and the Ethical Advisor at Karlstad University. In this section we describe the qualitative research methods employed, interview procedure and data analysis.

3.1 Participants

We recruited our participants via posting flyers around University of Pretoria's campus and asking individuals through word of mouth. In the invitation letter, we did not use the word "privacy" to avoid a bias. The invitation letter requested participants who had used any kind of car-to-car communication system, but did not place any other restrictions for participation. We asked all 16 participants that volunteered to first fill in a short questionnaire and sign a consent form for informing about data processing in compliance with POPI act and the GDPR. The questionnaire requested demographics (age group, gender, educational background) and asked them to specify the vehicular communication system they currently use or had used before. We interviewed 10 male (P1-2, 4-7, 10-11, 15-16) and 6 female (P3, 8-9, 12-14) participants in age groups ranged from 18 to 40, all from South Africa. Five participants were students (P1, 5, 9-11), 9 had a university degree (P3-4, 6-8, 13-16) and 2 had a MSc degree or higher (P2, 12). Our participants used different vehicular communication and navigation tools, most common Waze and Google Maps.

3.2 Interview Procedure

All interviews were conducted face-to-face in a semi-structured fashion, lasting for 20 minutes on average, and were all audio-recorded. Before we defined the catalog of interview questions, we conducted interviews with PET research experts of the field to identify the potential privacy trade-offs (see section 2.2).

Privacy perceptions and preferences for existing systems Particularly, the focus on existing systems rather than future developments was on purpose as we wanted to look at users' experience and perception on practical solutions and not on newer systems that are hardly in use or not at all. Participants were asked questions about their perceptions about existing vehicular communication systems in terms of perceived sensitivity towards location data tracking, location data linked with their identity, and if they want to manage and control the driving data or hand over the control to others. Furthermore, we asked them with whom they would share their identity/location data and with whom not, and whether the users would like that other drivers can have location privacy and under which conditions (e.g., whether accountability plays a role).

Privacy perceptions and preferences for PETs To address and identify drivers' trade-off preferences of short-lived pseudonyms, we asked participants questions about their perceptions in regard to different trade-offs of location privacy with costs, data quality/utility/usability, and safety. They were asked if they perceived any advantages of PET solutions for VANETs in comparison to existing ones, and whether they would pay for obtaining more pseudonyms from an issuing party to increase pseudonymity. They were also asked whether they would like to be located for safety reasons (in case of an accident), against whom they want to be private and whether they would like to have fine-grained privacy controls for protecting and sharing personal location data.

Privacy vs. data utility preferences We introduced participants with a use case for a privacy-enhancing solution based on obfuscation of location data. Practically they were said to imagine they were getting assistance from a navigation application on their mobile phone when searching for available parking spots in their nearby. They were shown two mock-ups consisting of two different navigation maps (see Figure 1), where in the first one the user would receive a map with parking places in the specific street he was interested in, and in the second one, he would receive a map with parking places for a larger region. In the first case, as he is the only driver in that street at the moment, the service provider can identify the user and see his fine-grained location. In the other one, it is possible to hide his exact location so that the system would not know where he is exactly, since there are many other cars nearby (it is possible to hide within a crowd of (k) other car drivers for achieving k-anonymity). Then, in order to get in the nearby parking spot, the user zooms-in the map. We asked them how they would trade privacy vs. data utility/usability in that scenario.

Ranking of goals In the last part of the interview, we asked our participants to rank different goals such as: usability and data utility, costs, safety, accountability, privacy.

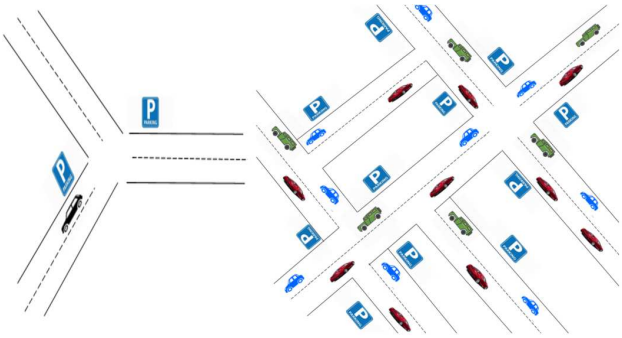

Fig. 1. Navigation maps mock-ups

3.3 Data Analysis

All interviews were audio-recorded, transcribed and coded using open, axial and selective data coding methods of grounded theory [12, 26]. Thus, the themes to answer the research questions emerged from the inductive analysis of the interview transcripts. To do so, we firstly got ourselves familiar with the data by reading through the scripts multiple times. Then we performed open coding process with the help of the guidelines from the Saldaña code book [25] to develop an initial codebook. Secondly these codes and concepts derived from the data were combined into categories and that resulted in the development of core categories in the axial coding phase. After iterative discussions between two researchers, we observed and agreed on a set of findings. Over 100 unique codes emerged from the analysis, which were then assigned to several categories such as "criteria for sharing", "data control", "lack of trust", etc. The data analysis was supported by NVivo 12 software. Using a software program such as NVivo facilitated creative management of multiple data sources, enabled multiple overlapping nodes and ensured visibility of our methodological processes [24].

4 Results

In this section, we present and expand on the main categories that emerged from the evaluation of the interview transcripts, including quotes from participants labeled P1 to P16.

4.1 Privacy perceptions about car-to-car communication

This category describes participants' perceived sensitivities and concerns about data used in vehicular communication systems, positive and negative perceptions using the system, and how they perceive location tracking implications.

Comfort with Data Collection Participants shared privacy concerns in regard to the system provider collecting personal data about them. Our analysis shows that perceived privacy and security risks of big data collection by the provider impacts their comforts. Six participants proved to be very uncomfortable with personal data being collected by the system. *"It actually scares me to know how much Google knows about me and the places I visit. There is a huge privacy issue there in terms of Google and in terms of what they actually track about the user. Cause as end users we do not necessary know what data Google is collecting and essentially what they are doing with that data"* (P2).

Ten other participants are less concerned about location data being collected, often rationalizing that it is beneficial to improve the system or the user experience. However, half of these participants (P1, 3, 9, 12, 15) are not comfortable with location data being linkable with other data, especially identity. This indicates that participants are often unaware that the user of location data can anyhow be easily identified, which means that they are anyhow concerned.

Therefore, all but five participants (P1-5, 9-10, 12-13, 15-16) would feel very uncomfortable with linking location data with name and that data being shared with third parties. *"I am on the edge about that because it is linked to my identity, that compromises my privacy"* (P10).

Furthermore, our observation demonstrates a lack of understanding of the problem of metadata that could be inferred from location data and thus, participants inadvertently believe there is no risk to privacy (P1, 8-9, 11, 13).

On the other side, P6-8, 11, 14 expressed different views on the perceived comfortability in respect to the third party the data is shared with, and the perceived benefits, as P14 argued: *"Well, I don't know. If it is insurance or somewhere I need help, then that is perfectly fine".*

Some participants (P3, 10-11) rationalized their reluctance to take actions to protect their privacy considering themselves not important enough, as captured by the following statement by P11: *"The only concern would be if someone wants to use my location data against me in some negative way, which I can not really see a situation like that happening except if I am the American president".*

When asked about the perceived level of sensitivity of different types of data such as: identity/location/navigation data, most participants (P1-4, 6-9, 12-14, 16) regarded them as very sensitive. *"I mean they are sensitive data, personal information so they are extremely sensitive to me"* (P12). In comparison, P5, 10-11, 15 do not really consider the data very sensitive.

Concerns about home address and identity information were among the most sensitive issues discussed, as partly mentioned due to burglary problems in South Africa. When asked if they think that someone could derive sensitive details from the location data, all participants identified home address inference concern. *"Generally no, but my house, my home yes. Like the data says I go to University of Pretoria every day that is fine but I don't want particularly people know where my house is"* (P9).

Moreover, some participants acknowledged that association of a user with a specific location can reveal sensitive details about different things: health prob-

lems, association among people, habits, etc. *"Yeah, definitely, I mean you can figure out if two people are closely related, you can figure out when did they meet up, where they meet up"* (P16).

Users privacy concerns in car-to-car systems Privacy risks can be conceptualized as the perceived potential loss of control in regard to data disclosure and the potential misuse of personal information [29].

Participants' privacy concerns range from fear of data misuse and worries about bad privacy practices of the data in general, to data security issues and potential leaks. Among the perceived risks they emphasized the risk of tracking, profiling, third party data sharing and impersonation attacks.

Most of the participants (twelve out of sixteen) fear that their data could be used in a way that could damage their reputation and perceive location tracking implications in terms of privacy and safety, often aggravated to fear of life. *"I do think there are implications if someone is looking to do something malicious then yeah, definitely. As I said if someone is willing, they can put in the effort and try to track me down"*(P10). On a related note, three participants (P9, P10, P13) raised the fear of stalking as a possible implication of tracking. *"I mean of course someone can find where I stay and use that against me by coming to my house or following me where I would go usually everyday, I could be stoked"* (P9).

Several other participants (P5, 11-12) identified location tracking implications in relation to car robbery crime or safety threats in South Africa. *"For instance I know criminals in South Africa especially try to keep track of when someone is at home or when they get back. If they then get my information and keep track of when I am not home to possibly go and rob, yeah"* (P11).

P12 emphasized the safety risks of kidnapping: *"Of course there is security implication, especially in South Africa, you wouldn't want anyone to know where you are living because the problem is in terms of security, is the people that know you that actually are the security risk and not the people that might not know you. To an extent for example in my home country kidnapping is a huge thing".*

Some participants highlighted their inability to prevent location tracking by keeping the location disabled as much as possible and seem resigned against constant tracking by companies. *"I guess you just resign to the fact that Google can do this much tracking and damage to your reputation, you come to terms that being the only option that you have"* (P2). P12 has lost her trust in achieving location privacy noting: *"I know I am being tracked and I know there is no privacy so I don't. . . ".*

On the other side, participants expressed concerns whether companies have the adequate technical means to protect their data, whether it is stored securely, encrypted and anonymised in the first place. Moreover, users are concerned of the purposes the driving data is being used for, as highlighted by P16. *"It would be quite intense I think because it sort of comes out to how would they use that information, that would be my biggest question"*. Regarding other factors impacting their concerns, participants (P1-2, 6) echoed issues if data leaks or

gets hacked and gets into wrong hands (criminals). *"Maybe I don't want to use this because I don't want this data to be leaked to anybody"* (P1).

Managing data collection is very difficult for users because of the different collectors, which challenges the users' trust regarding intentional or unintentional collection of information that is not necessary for the service. P12 brought up the problem of the enormous data that is collected and its potential misuse from the services in South Africa. *"How much unnecessary information they would collect for every service in South Africa, the purpose that they collect it for is not what they use it for, but are trying to use it for personal gain. In such scenario I am not protecting my privacy but I feel that they are invading my space"*.

If the data is collected, it is easier for the external entities, collectors, governments, hackers to access and use the information. Especially, participants identified an increasing potential for data exploitation by government and law enforcement, hence feeling about potential privacy intrusions.

Trust on external entities Data disclosure means loss of privacy, hence it is translated in loss of trust by many participants (P1, 3, 4, 7, 10, 12, 16). Our results demonstrate that some participants (P4, 7, 10, 13) often perceive strong lack of trust towards service provider companies and their data collection and handling practices. *"I wouldn't trust companies, I don't know why I trust them"* (P7). Our analysis identified that participants are very concerned about the probability of data misuse by the data receiving party and previous research found out that users with high privacy concerns also mistrust the integrity of service providers to appropriately handle their data (Zhou, 2012).

Furthermore, benefit or threat to privacy depends also on the entities that gain access to personal information, thus participants perceive different division of trust level between many entities. For instance, all participants identified their trust in family and friends, but not necessarily in government as highlighted by P2 and P7. *"I think anybody or government that want to exploit data in terms of spyware or tracking users based on certain risk factors or bodies that want to sell the information to make profit"* (P2).

On the other side, some participants (P3, 8-9, 15) perceived trust in location based service provider, but do not want to release the data to the public or to share it with other third parties.

In comparison, the results could also replicate a significant negative effect of privacy concerns on trust on other drivers in regard to the location data. When asked whom would they trust in respect to location data, many participants (P1-2, 4-5, 7, 16) declared they would not trust anyone. *"I don't know whom I wouldn't trust because well, you just don't know, you just don't trust anyone in general"* (P1).

4.2 Preferences for PETs

This section describes users' privacy preferences in regard to identity management control options, it provides a detailed overview of participants' requirements in regard to collecting and sharing the driving data, conditions for being

tracked, and whether they prefer other drivers to have location privacy and under which conditions.

Trust in PETs Our interviewees (eleven out of sixteen) recognize the benefits of short-lived pseudonyms and PETs in terms of enhancing data privacy, enabling anonymity, and protecting against tracking and profiling. However, P2 and P12 indicated they would trust pseudonymity only if traceable in case of crime, if accountability is guaranteed. *"I am definitely in favour of the privacy-preserving pseudonyms however, I guess there is a case where we have to forsake some sort of trade-off to actually have some regulations and laws in place, so if certain incidents happen you should actually be able to track an attacker for instance but, it should not be overly exploited by law enforcement for spying"* (P2).

Other participants (P6-8, P10) reflected on other advantages of PETs in regard to protecting against tracking and profiling. P9, 11, 14 confirmed they would feel more secure and safe with PETs as they believe PETs can protect users (scared of being assassinated) from malicious people. P4 liked PETs but he believes they can be in conflict with transparency: *"I can see advantages like security but then also if you want to see the data they have on you, that would be very difficult if it is more security in place. You can't track your data and staff"*.

However, some participants perceive limited trust that PETs can protect location privacy. For instance, P1 had issues trusting that pseudonymity is securely implemented, and P2 stated that trust in PETs requires open source. Several other interviewees also had some questions in regard to PETs. While P14 seem to have doubts how far databases can really be secured, P16 is not sure how privacy controls can be implemented.

Privacy preference specification Our qualitative analysis indicates that participants have different perceptions in relation to data control, most of them (nine participants P1, 4-5, 7-8, 11-13, 15) prefer to hand over the control to a trusted third party believing that they are not inclined to manage the data as it may be difficult, time-consuming or may hinder system's usability. Given their desire for convenience and the difficulty to configure privacy settings, participants might instead trust the service provider to protect their privacy. Previous literature has shown that users may be unwilling to manage their privacy due to the required effort to manage privacy controls and the perceived difficulty to configure them [19]. In comparison, seven participants (P2-3, 6, 9-10, 14, 16) desire full controls over the data they share, from decisions to who they share it with, data minimization to rights to deleting collected data. *"I would say the least amount of driving that that being collected is the best, so I would like to have full control of my driving data or any data that is being collected"* (P2).

All but three participants (P8, P11, P15) prefer fine-grained privacy control options for protecting and sharing personal location data.

Moreover, participants want to be granted control such as the option to access, to consent or deletion of their data. Several participants (P5, 16) emphasized that users should be able to delete the data collected about them. P5,

12, 14-16 strongly seek to consent for any data processing practices and want to have their right to data traceability. P12 explained, *"I prefer to know and let me give my consent to say you can go ahead and use it for research or whatever but, let me be aware of it"*. In addition, participants (P2, 5, 12) desire to be notified and aware of location tracking. Some of them (P3, 6-8, 14) are comfortable to be tracked by insurance companies and sometimes police only if it is transparent and there is a need. When asked whether they want to be tracked for safety, in case of an accident, P2, 5, 11-13 identified the option to share location in distress through a panic button rather than being constantly tracked while driving. *"Give you the option to share that, let's say there is a button that says: Emergency, call the police"* (P5). Furthermore, P10 explained that he refuses to be tracked by companies: *"I think I don't mind being tracked by close friends and family but I don't think tracking information is necessary to big companies and stuff like that"*. Some interviewees (P2, 5, 7) noted they dispel spying by government or police. *"I wouldn't like to be tracked by the police or things like that"* P(5). Other participants (P1-2, 9, 12) stated they dispel being tracked at all, probably due to the identified safety risk in South Africa. *"I don't want anyone to track me. Nobody should track me, no one"* (P12).

Transparency Transparency relates to the legal right of the data subject, granted by the GDPR and the POPI act, to obtain insight in regard to all processing practices of his data by the data controller. Transparency about the data collected and the purpose of the collection also influence comfort levels for data collection [2]. In light of our findings, transparency was a key concern shared by participants, both in terms of data collection, the processing and storing of it. This concern increases when data is shared with third parties as P2 elaborated: *"Sometimes is not really transparent in terms of end user knowing that this is actually happening, without reading through the long terms and conditions to find print where they say that they store some information about you. It could be sending it off to third party companies to get additional revenue profits, so there is no transparency or accountability in terms of what Google is doing with this location tracking"*.

Insights from the responses indicate that participants perceive a strong lack of service provider accountability, and several of them (P2,12) relate to the GDPR, raising an interesting point in regard to the applications often being not fully GDPR compliant with the principles of data minimization and transparency. Some interviewees also noted that while the collected data would not necessarily be misused, the uncertainty of what happens with it actually concerned them more. In principle, all but two participants identified they explicitly seek transparency for the collected data. A strong requirement that participants have is to be aware of the data that is collected about them. This includes to be informed about which kind of data are collected, who is receiving it and what is done with it. *"I would like to know who is being able to see it and why they need to see it"* (P9).

Our analysis suggests that participants (P2-5, 11-12) are particularly strict about seeking transparency of purposes of data use, as P12 put it: *"I want to know what my data is being used for, and if it is being used for what is said they want to use it for"*. P4 and P14 demand transparency not only of how data is handled, but also and if it is secured and whether it leaks. P8 also pinpointed transparency in regard to breach notifications, noting: *"I would like to know if there has been any leaks"*.

Even though participants prefer to be informed about everything, this is practically not always the case, as explained by P1-2, 4-5, 15, who complained about privacy policies often being too long, containing irrelevant information or difficult-to-understand.

Sharing criteria We analysed participants' preferences in regard to with whom they would like to share their identity/location data and with whom not, and whether participants would like that other drivers can have location privacy or not and under which conditions. Through the responses related to discomfort of data collection, we found out many factors of why participants do not want to share their data. Perceived risks and limited trust on external entities to protect the data, were key observations to impact participants' unwillingness towards sharing their driving data.

In contrast, most of our participants (12 out of 16) pointed out they would share location with family and friends. Noteworthy is that participants showed a high agreement in regard to the specific cases they would share the data other than their family members.

Participants mentioned safety or emergency situations as the only purposes for data sharing that they would approve of. When asked whether they want to share location or identity in case of an accident, all participants expressed willingness to share location and identity for safety reasons. Therefore, ten out of sixteen participants indicated they would share location with law enforcement or insurance for emergency services. However, they seek to share location by choice, expose it only when the need arises and not continuously while driving. *"Yes, but it would have to be a choice, I would have to say I am at this location, I would have to give consent that someone else could access it"* (P16). On the other side, the perceived limited trust to use the data appropriately would make some participants (P1-2, 15, 16) hesitant to share location or identity with external entities for safety situations. *"Yes, if I have a confidence that that is what it is used for I guess. If I can guarantee that they are going to use it in a responsible way"* (P15). Our results further substantiate this, as some participants (P2, 7) seek to be private against government and law enforcement and many (P4, 7, 10, 13, 16) conveyed that they want privacy against companies.

Other participants (P1, 3, 10, 13-14, 16) expressed they want other drivers to have location privacy as well, and they also liked their family members to be locatable for safety reasons. *"As well as emergency services, yes. I have a younger brother, he is still sixteen and when it comes to certain things, you would want to know where they are"* (P13).

4.3 Privacy trade-off preferences

This section reports about participants' willingness to trade privacy for data utility, safety and costs.

The wish for increasing safety and the wish for privacy and potential trade-offs, is seen in two different spectrums, safety from criminals and hackers, and traffic safety against car accidents. We found out that the higher the perception of safety risk from car accidents, the likelihood to trade privacy among participants increases. All of them agree to share location for traffic safety.

In contrast, our results exhibit significant effects of car robbery problems in South Africa on the desire for safety and protecting one's own privacy. Participants showed strong safety concerns particularly in regard to tracking for criminal purposes, kidnapping and stalking (see Section 4.1), thus they explicitly demand location privacy from criminals and hackers. Hence, location privacy towards the service provider and other drivers is rather perceived as an important enabler for safety against criminals. While conflicts between privacy and safety still arise in regard to the question if the drivers' location should be kept private from law enforcement, most users would still only trade-off privacy in specific emergency cases due to their limited trust, as discussed above.

Our results also indicate that many participants (P2, 7-8, 11-13) acknowledge the importance of user accountability.

The perceptions of privacy risks to personal data had considerable impact on participants that were less likely to trade privacy off with data utility. Ten out of sixteen participants precised they would not trade privacy off with data utility/usability. When asked about the use case presented to them (see Section 3.2), participants (P3-6, 8-10, 13-14, 16) expressed they would be interested in a more privacy-friendly solution on the cost of data utility/usability. *"I go for the second one cause my data is protected. And I think it wouldn't take much time for me to be able to zoom in and try to get my parking place that I am looking for"* (P6). P5 regarded location privacy more important than usability in the context of safety problems in South Africa. *"I think the second one, just in terms of I wouldn't want people to know where my car is and to be able to follow me because in our case in South Africa maybe it is a dangerous area where I am looking for a parking spot and they will know where I am and that I am going to be there"*.

However, not everybody perceived the map providing location generalisation as a trade-off. P8 would actually see bigger utility on the bigger map, explaining: *"I would prefer the second one actually just because it gives me an overview of..., I would like to see in my nearby region where the parkings are rather than just one specific region"*. Insights from the responses indicate that the higher the perception of convenience among the other participants (P1-2, 7, 11, 15), the likelihood to trade privacy increases. *"First of all, it makes sense, it is pretty cool. I would probably be on the convenience side and sacrifice privacy but I think the beauty of this thing is you can be on a continues spectrum, depending on how much you value privacy and the granularity of this. But for me personally I am on the convenience side"* (P15). In contrast, P11 saw it in relation to crime

problems in South Africa: *"So, in terms of this, I would say, especially in South Africa, the first one, the utility is much better cause people in South Africa tend to park very close to where they want to go cause they are scared to walk".*

Only one participant, P12 explained the trade-off between usability and privacy depending on the context: *"I am willing to trade-off if the need arises, and the trade-off for me is really important. But at any given space, the trade-off will always win: what is more important to me right now? Do I need a parking now or do I need to protect my privacy now? When I weight the options, I choose what works now. Tomorrow I may decide not to came to campus by car. I turn off the tracking and I walk, so it depends".*

However, when asked to rank usability, cost, privacy, safety, accountability and driving assistance (data utility) as essential triggers of introducing privacy-enhancing solutions for vehicular communication in the future, there was no clear indication of their preferences, as participants showed a high variance in their rankings and also in relation to the above use case preferences. For instance, six participants (1-2, 9-11, 16) valued usability the most relevant goal, while four participants (P4, 6, 10, 13) ranked privacy the highest goal and four other participants (P3, 5, 10, 14) ranked safety against criminals on top. While three participants (P7-8, 15) qualified driving assistance (data utility) the paramount goal, interestingly, only P12 perceived accountability the most important. It is important to note, that privacy, usability and safety were perceived nearly at the same level, as participants perceived safety and privacy equally important as their second option.

In light of our findings, cost was perceived the least important goal by all participants. When asked if they would be ready to pay more for more frequently changed pseudonyms issued by a third party, we observed a split in participants' attitudes towards paying. The majority of them (9 out of 16) stated they would not pay for short-lived pseudonyms. Within the qualitative responses related to hesitance to pay for more short-lived pseudonyms, we also found explanations of why participants do not want to pay. P2 and P5 rationalized their reluctance by inferring that pseudonymity/privacy should be cost-free. *"Generally this anonymity I think shouldn't really come at the users expense because then you kind of discriminate against users in terms of - if you want to be more secure you have to pay more"* (P2). *"The thing is I wouldn't want to pay for it because that is going to send various people to be less safe because people want the free option"* (P5). While P9 (wrongly) thinks that three alternating pseudonyms would be sufficient to protect her identity, P12 anyhow does not trust pseudonyms, as she thinks that they could still be linked with her name. While most participants expressed scepticism to paying, some (P3-4, 6, 10, 13-14) noted they were willing to pay but not to a large extent.

5 Discussion

In this section, we discuss the results in terms of the cultural impact and in terms of end user and design requirements that we can derive for privacy-enhanced VANETs. Moreover, limitations of our study are briefly discussed.

Cultural aspects: We believe that several of our findings are specific for South Africa and may not apply for users or other countries, such as especially demand for location privacy for protecting against criminals and stalkers, which is more an issue in South Africa than Sweden. In addition, also the lack of trust in Government does likely differ from Sweden, which is according to a recent Eurobarometer survey the European country with the highest trust in government in regard to handling its citizens' data [9]. Moreover, the willingness to share location information with family and close friends may be different from Sweden that has been classified as an individualist society [14] in which responsibility is taken for direct family only and in which family bounds may be less tight.

End user and design requirements: From our findings we can derive requirements for privacy and identity management for VANETs. Firstly, given the users' desire for transparency and control, transparency and intervenability online functions should be offered by design. Particularly, for VANETs based on short-lived pseudonyms, there should be options for the users to securely and pseudonymously exercise their transparency and interveneability rights online (e.g., by authenticating users as the pseudonym holders with zero-knowledge by using anonymous credential proofs [4]), as it is for instance also supported by Art. 11 (2) GDPR. Secondly, for meeting preferences in terms of data sharing as stated by the study participants, fine grained controls should allow to share location data with persons of trust, while restricting access for the provider and other external parties. Thirdly, different selectable profiles of privacy settings should be offered for South African users. The default setting should enforce the most privacy-friendly option for enforcing the privacy by default principle. In addition, further selectable profiles could differ in regard to different degrees of privacy trade-offs with utility/usability and costs while not compromising on traffic safety and basic privacy protection that were rated with highest priority.

Limitations: Our study may have a bias through the limited number of interviewees with higher educations than the average population. Also for this reason, we plan a follow-up quantitative study for analysing hypotheses derived from this study with a broader sample of participants.

6 Related Work

Previous surveys reviewing privacy-preserving solutions for IoT environments and VANETs based on pseudonyms [1, 23] show that while there have been an extensive research focusing on technical aspects of PETs for vehicular communication systems, the end-user aspects of such systems, and especially usable

pseudonym configurations considering privacy trade-offs, are still fairly unaddressed. Nonetheless, earlier research has treated the users' privacy perceptions and requirements for different IoT application areas, especially for smart homes, and for mobile applications, or have studied related end user aspects concerning privacy and trust for VANETs.

Previous related studies on smart homes have also focused on end user privacy perceptions and requirements. For instance, the authors in [35] examined users' attitudes regarding privacy, intimacy and trust issues for medical technology in smart homes and found privacy and trust the main requirements of users. Another work [32] explored user-centered privacy design for smart homes and identified usability, user experience, system intelligence, system modality and, similarly as we identified in our study for VANETs, also data transparency and control, security and safety, as key design factors for smart home privacy. Cottrill et al. [5] conducted a survey to examine consumers' perceptions of privacy in the mobile environment and also researched location data sharing preference factors. The results revealed that while participants responses perceive that sharing data in the mobile environments pose privacy risks, they do not take further steps to protect their privacy. Moreover, key findings were that users' privacy preferences and willingness to share location data are impacted by personal characteristics, contextual factors of the possible sharing of data (entities the data could be shared with - which is also discussed in our study), and the perceived benefits.

In the vehicular context, [31] examined the acceptance of connected vehicular services in a high-fidelity simulation environment and observed privacy perceptions to impact usage adoption. Bossauer et al. [3] qualitatively analyzed the relationship between the need for trust and privacy in peer-to-peer car-sharing from the perspective of car owners and rentees. Though, not exclusively focused on privacy and vehicular communication, a related set of research [34, 33, 20] have investigated users' perceptions on privacy concerns and preferences inside the smart home environments and have identified a range of findings, highlighting the importance of understanding users to be able to create usable privacy mechanisms [15]. Others have also shown in an empirical study similar findings in regard to users' perceived privacy concerns for connected cars in terms of a lack of transparency of data sharing with and use by car manufacturers [27]. This work also reports that some study participants mentioned perceived benefits in terms of safety and risks if location data are shared with the police or household members for tracking activities, without that this work is however analysing these aspects more systematically and in more detail.

Despite such previous work examining end user aspects for other IoT and mobile application areas, to the best of our knowledge, this study is the first to analyze drivers' privacy perceptions and preferences for privacy trade-offs and control for privacy-enhancing car-to-car communication systems. Moreover, we are the first to study these end user aspects for VANETs for South Africa.

7 Conclusions

In this paper, we reported on a qualitative study on privacy perceptions and preferences for deriving requirements related to privacy-enhanced car-to-car communication systems. We asked 16 drivers from South Africa about their preferences about control and trade-offs of PET solutions for vehicular communications. The main results and key observations that strike us as the most vivid and representational of the study for South African users are listed below in relation to our two research questions that they are addressing.

Recurring themes answering RQ1:

- The more sensitive the data are perceived, the more concerned, the less willing the users are to share.
- Participants are uncomfortable of location data being linked with their identity.
- Drivers often perceive lack of trust on external entities (government, police, ISP) to protect their privacy properly.
- Drivers perceive limited trust in the privacy protection of PETs.
- Participants want more control over their privacy and want to make privacy decisions transparent (usable privacy notices and control, transparency and fine-grained settings).
- All of them are willing to share location and identity with family and close friends.
- All participants are willing to share location in distress, they dispel being tracked all the time.
- Drivers want to remain private against other drivers.

Recurring themes answering RQ2:

- Safety against criminals and privacy are the primary concerns of drivers in car-to-car communication systems.
- Participants perceive safety implications (from criminals, hackers) of location tracking.
- Opinions about data sharing depend on perceived safety benefits and trust on external entities.
- Convenience (usability), privacy and safety (both traffic safety and safety against criminals, hackers) are top priorities for users.
- Some participants are willing to pay for pseudonyms, but not much.

Based on our findings, we also elicited a first set of design requirements for usable privacy and identity management for VANETs. Participants demonstrated different views on location data sharing, and hence, different selectable profiles should be offered based on different degrees of privacy-trade-offs with utility/usability and cost. Moreover, transparency and interveneability options should be offered by design, also for pseudonymous users, and fine-grained control options should be available for users.

We are currently conducting the same type of interviews in Sweden for an intercultural comparison and gaining further insights in regard to how far selectable profiles of typical preference settings should differ for South African and Swedish drivers. This will allow us also to derive hypotheses that will be tested with a quantitative study for a follow-up in-depth analysis.

Acknowledgements

This work was supported by the Swedish Foundation for Strategic Research (SSF) SURPRISE Project and the South Africa-Sweden University Forum (SASUF). We would like to thank all interview participants and our partners from the SURPRISE project that contributed with valuable background information.

References

1. Akil, M., Islami, L., Fischer-Hübner, S., Martucci, L.A., Zuccato, A.: Privacy-preserving identifiers for IoT: A systematic literature review. IEEE Access **8**, 168470–168485 (2020)
2. Bilogrevic, I., Ortlieb, M.: " if you put all the pieces together..." attitudes towards data combination and sharing across services and companies. In: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems. pp. 5215–5227 (2016)
3. Bossauer, P., Neifer, T., Stevens, G., Pakusch, C.: Trust versus privacy: Using connected car data in peer-to-peer carsharing. In: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. pp. 1–13 (2020)
4. Camenisch, J., Lysyanskaya, A.: An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In: International conference on the theory and applications of cryptographic techniques. pp. 93–118. Springer (2001)
5. Cottrill, C.D., et al.: Location privacy preferences: A survey-based analysis of consumer awareness, trade-off and decision-making. Transportation Research Part C: Emerging Technologies **56**, 132–148 (2015)
6. Da Veiga, A.: An information privacy culture instrument to measure consumer privacy expectations and confidence. Information & Computer Security (2018)
7. Da Veiga, A., Ophoff, J.: 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. pp. 16–29. Springer (2020)
8. Dala, P., Venter, H.S.: Understanding the level of compliance by south african institutions to the protection of personal information (popi) act. In: Proceedings of the Annual Conference of the South African Institute of Computer Scientists and Information Technologists. pp. 1–8 (2016)
9. EU Commission: Special Eurobarometer 431 – Data Protection (2015)
10. EU Commission: Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union **L119**, 1–88 (2016)
11. Garidzirai, R., Chikuruwo, R.E.: An economic analysis of the social grant policy in south africa. Journal of Advanced Research in Law and Economics **11**(2 (48)), 362–369 (2020)

12. Harry, B., Sturges, K.M., Klingner, J.K.: Mapping the process: An exemplar of process and challenge in grounded theory analysis. Educational researcher **34**(2), 3–13 (2005)
13. Heid, B., Huth, C., Kempf, S., Wu, G.: Ready for inspection: The automotive aftermarket in 2030, https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/ready-for-inspection-the-automotive-aftermarket-in-2030, (accessed: 13.09.2020)
14. Hofstede Insights: Country comparison, https://www.hofstede-insights.com/country-comparison/sweden/, (accessed: 13.09.2020)
15. Jacobsson, A., Davidsson, P.: Towards a model of privacy and security for smart homes. In: 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT). pp. 727–732. IEEE (2015)
16. Jin, H., Papadimitratos, P.: Resilient privacy protection for location-based services through decentralization. ACM Transactions on Privacy and Security (TOPS) **22**(4), 1–36 (2019)
17. Khodaei, M., Jin, H., Papadimitratos, P.: Secmace: Scalable and robust identity and credential management infrastructure in vehicular communication systems. IEEE Transactions on Intelligent Transportation Systems **19**(5), 1430–1444 (2018)
18. Lunheim, R., Sindre, G.: Privacy and computing: a cultural perspective (1994)
19. Madejski, M., Johnson, M., Bellovin, S.M.: A study of privacy settings errors in an online social network. In: 2012 IEEE International Conference on Pervasive Computing and Communications Workshops. pp. 340–345. IEEE (2012)
20. McCreary, F., Zafiroglu, A., Patterson, H.: The contextual complexity of privacy in smart homes and smart buildings. In: International Conference on HCI in Business, Government, and Organizations. pp. 67–78. Springer (2016)
21. Papadimitratos, P., Gligor, V., Hubaux, J.P.: Securing vehicular communications-assumptions, requirements, and principles (2006)
22. PARLIAMENT of the Republic of South Africa: Protection of Personal Information Act (POPI Act) (2020), https://popia.co.za/, (accessed: 15.10.2020)
23. Petit, J., Schaub, F., Feiri, M., Kargl, F.: Pseudonym schemes in vehicular networks: A survey. IEEE communications surveys & tutorials **17**(1), 228–255 (2014)
24. Ryan, M.E.: Making visible the coding process: Using qualitative data software in a post-structural study. Issues in educational research **19**(2), 142–161 (2009)
25. Saldaña, J.: The coding manual for qualitative researchers. Sage (2015)
26. Strauss, A., Corbin, J.: Grounded theory methodology. Handbook of qualitative research **17**(1), 273–285 (1994)
27. Svangren, M.K., Skov, M.B., Kjeldskov, J.: The connected car: an empirical study of electric cars as mobile digital devices. In: Proceedings of the 19th International Conference on Human-Computer Interaction with Mobile Devices and Services. pp. 1–12 (2017)
28. Sweeney, L.: k-anonymity: A model for protecting privacy. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems **10**(05), 557–570 (2002)
29. Tan, M., Teo, T.S.: Factors influencing the adoption of internet banking. Journal of the Association for information Systems **1**(1), 5 (2000)
30. Venter, E.: The notion of ubuntu and communalism in african educational discourse. Studies in philosophy and education **23**(2-3), 149–160 (2004)
31. Walter, J., Abendroth, B.: On the role of informational privacy in connected vehicles: A privacy-aware acceptance modelling approach for connected vehicular services. Telematics and Informatics **49**, 101361 (2020)

32. Yao, Y., Basdeo, J.R., Kaushik, S., Wang, Y.: Defending my castle: A co-design study of privacy mechanisms for smart homes. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. pp. 1–12 (2019)
33. Zeng, E., Mare, S., Roesner, F.: End user security and privacy concerns with smart homes. In: Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017). pp. 65–80 (2017)
34. Zheng, S., Apthorpe, N., Chetty, M., Feamster, N.: User perceptions of smart home iot privacy. Proceedings of the ACM on Human-Computer Interaction **2**(CSCW), 1–20 (2018)
35. Ziefle, M., Rocker, C., Holzinger, A.: Medical technology in smart homes: exploring the user's perspective on privacy, intimacy and trust. In: 2011 IEEE 35th Annual Computer Software and Applications Conference Workshops. pp. 410–415. IEEE (2011)