Human-Centric Design of Privacy Controls for Autonomous Vehicle Data Sharing

By Dr. José Barreto

Professor of Informatics, University of Lisbon, Portugal

1. Introduction

Societal concerns need to be different—those resulting from driver fears associated with data cameras in a smartphone, thus restricting the information sharing and autonomous driving, self-driving vehicles, driver control, and these two technologies taken together. It is also essential to differentiate these technologies. It is very clear now that evidence-based studies demand the wide-scale application of autonomous technologies. This demand emerges from societal, economic, and technological perspectives. It is recognized that long-term development of automated technologies is urgently expected to accelerate safe data sharing and to promote collaborated global research. To transfer the technology similarly into reality, promoting the preparedness of interested users' vehicle data management and the overall infrastructure through consensus building has become an critical priority [1].

Driver privacy is an emerging critical concern in connected vehicular systems [2]. The concern arises in relation to personal information protection, location information, driver data privacy associated with various sensors such as cameras, third-party sharing consent issues, social applications of all such data, and privacy-related user choices. Various privacy issues are separately discussed in different articles [3]. A connected vehicle community, particularly automotive and infrastructure researchers, system designers, and regulators, must intervene to address the above privacy challenges competently. In the immediate few years of new technologies, attention must be devoted to regulating, contextualizing, and perceiving the privacy issues in vehicular environments in a wider context. A few efforts to secure the above privacy issues demand confidentiality (driver) and mapping of individual privacy expectations of data sharing.

1.1. Background and Significance

Privacy concerns and related challenges are evident from the fact that vehicle crash information recorded in vehicles solitary can be used as evidence to support legal verdicts on accidents occurring around driving context. Internet-of-Vehicles (IoV) also induces privacy concerns with multiple vehicles, device-to-vehicle communications. Recent prominent issues with privacy protection of IoT data prohibit design simplicity and restrict data sharing rules among DSUs comprising of multiple data providers and data consumers [4]. This is mainly because data protection and privacy must permeate throughout the data management lifecycle and procedures to be privacy-centric from the standpoint of the original data recording itself. Enhancing privacy preservation with modern SDVs involve autonomous data sharing, obstruction with data functionality and accuracy [5].

SDVs (Self-Driving Vehicles) are becoming an integral part of our road infrastructure with the potential of reducing mobility impairments, fatalities, and economic burdens caused by human error-based accidents [6]. On the flip side, SDVs manage, transmit, and process a variety of data with significant privacy implications. The vehicle itself collects, processes, and records an enormous quantity of personal statistics using various sensors. The information may traverse in and out of vehicles connecting to various services enroute. Vehicle-to-vehicle, vehicle-to-infrastructure, and vehicle-to-third party communication protocols manage to transmit data interaction with various autonomous, semi-autonomous, and human driven vehicles.

1.2. Research Objectives

Our results help to reduce the knowledge gap and provide a deeper insight into an appropriate design and deployment of privacy controls for autonomous mobility systems. We support the realization of privacy-friendly mobility solutions by contributing the "privacy canvas", practical guidelines for theory-based AV privacy design, and original AV-related privacy values regarding various AI-based system requirements [1]. Given the need for a privacy-sensitive data sharing ecosystem in the context of autonomous vehicles (AVs) and in the absence of a standalone open-source simulation environment specific to such a data-sharing scenario, we propose an open-source toolkit that is designed exclusively for simulating privacy-sensitive aspects of autonomous vehicles. It is flexible, extensible for supporting additional agents and tasks and incorporates scenario-relevant risk detection mechanisms pertaining to AV data sharing and privacy [5].

RQ4: How will the inclusion of a privacy management mechanism in an AV influence behaviour, use-case valuations, attitudes towards privacy and acceptance of the vehicle? (Chapter 6)

How do we account for differences in situational awareness, user knowledge, and technological competence when designing privacy controls for AV data sharing? (Chapter 5)

RQ1: How can we design privacy controls for AV data sharing that are aligned with people's privacy preferences (e. g., individual privacy needs and usage-related privacy requirements)? (Chapter 3) RQ2: How do we take into account broad socio-technical conditions under which AVs may be deployed so as to satisfy diverse stakeholder privacy preferences while accounting for adverse effects such as privacy fatigue, which potentially threaten uptake of, and dependability on, AVs? (Chapter 4) RQ3:

In this thesis, we aim to develop a human-centric privacy control system for AV data sharing [7]. We set out to address the following research objectives captured in the following research questions:

2. Autonomous Vehicles and Data Collection

Vehicular networks, when exploited to provide search, navigation, and other services to ISDs, might become a significant source of new data collection. Here, we refer to any system that might centrally collect vehicle data for any purpose as CAVD. The data is also already collected in the practice of pandemic control. Adversaries can directly perform real-time and post-incident surveillance of specific vehicles, indirectly collect detailed accident site surveys, and collect driver distribution surveys to ultimately conduct killings, sharpening between to rare subforms using cursed attributes on public transporters are campuses [8].

There has been a significant amount of research focused on the general privacy concerns of autonomous vehicles (AVs) [6]. The issues cover data ownership, data storage, data sharing, data usage, data control, data consent, and data access. The AV data might include large-scale, microscopic data (i.e., detailed data about the conditions of specific places) that can be used against individuals. The data might as well include data that allows making inferences about personal health, like who visits cancer care centers [9]. The data is stored and updated over and over, possibly for years. So, inferences about the sensitive information that can then be

made with the algorithms that are trained over years will potentially become more and more precise over time.

2.1. Overview of Autonomous Vehicle Technology

The autonomous vehicles (AVs) of the near future will be equipped with advanced features and monitoring measurement systems. Vehicles will obtain data from various types of sensors. The data may include driving trajectories, including velocity, acceleration, and position [2]. Along with such basic information, the data may also concern operational settings, fuel and energy management; the status of mechanical parts, engines, and batteries; data on autonomous and assisted driving; as well as data on health monitoring. The control and comfort of the passengers and their driving experience closely depend on the data collected by the vehicle. From the point of view of improving the comfort of driving, increasing driving safety and control, as well as reducing fuel and energy consumption, this aggregated vehicle-collected data could significantly support many smart mobility functions, which directly concern driver control [6]. The collected data also have various second lives. These secondary data usages can support many smart and personalized mobility services. These can be the optimization of EV charging and driving, autonomous or semi-autonomous driving functions improvement, the improvement of navigation systems with traffic prediction and alarming warnings (e.g., heavy braking, city alerting, situations without visibility, etc.); additional personalized driver assessments and monitoring (as a kind of game remember an eco-drive). The data can be shared to improve a social quality of life service, such as a noise map, pollution map services, or have an assessed value in car sharing or parking situations. Car sharing companies already use vehicle-collected data and have interest in car user behavior monitoring, parking places prediction, demand for car sharing, and preferred zones of movement. Privacy concerns about the third-life data usage are also included in works on new privacy-friendly solutions for digital mobility. Fleets of AVs connected in smart cities could share vehicles' data in a controlled and privacy-compliant way offering a unique and complementary data source for roads monitoring and maintenance. Such data usages could help to improve road conditions, control the life-cycle status of the road properties, road safety, develop smart traffic management, and improve predictive analytics in transportation policy modeling. The smart mobility concept relies directly on solutions using vehicle-collected data, but at the same time, vehicle-collected data could

become a digital freight for case studies on a new privacy model concerning shared data on the road net; and in this context still a gap exists and needs a coherent solution.

2.2. Types of Data Collected

Processing this raw data, utilizing advanced computation techniques and algorithms result in data that can be assumed to be of high quality and ideally private and secure, depending on the approach that was followed for its generation. Meanwhile, both datasets are of potential advantage to third parties, possibly creating undisclosed privacy and security risks at both the individual and the population levels. Different strategies and measures need to be applied to adequately secure and privacy protect raw and processed data.

For each of these types of data, we attempt to detail the potential security and privacy concerns. Raw data collected by CAV's IoT sensors' networks; in particular, information collected by cameras are more prone to privacy risks and concerns that put the occupants' privacy at risk [10].

The data shared and transmitted in and among connected autonomous vehicles can contain information pertaining to various domains: Regular data collected by vehicle sensors through Internet of Things (IoT) and other wired or wireless communication channels, and extra data that provide useful insight about the surrounding environment of the vehicles. From a security and privacy perspective, we will categorize the data that can be collected in two primary categories, namely, raw data collected by IoT sensors and processed data in the form of maps that will add to the environmental understanding at the V2V level [7]. Figure 1 illustrates the taxonomy.

3. Privacy Concerns in Autonomous Vehicle Data Sharing

Vehicle-to-everything (V2X) features modernize currently operational self-rider vehicles by sharing their raw diagnostic, driving, and location position data to an off-vehicle server for analysis of patterns, real-time monitoring, abnormality alerts, and other uses [3]. At the same time, enforcing an entity for that off-vehicle server to collect data from different AVs simultaneously and either with drivers or driverless trends will improve shared road security. As AVs shifts into a smart transportation schema, they are becoming more connected with each other in a sense where they work together. A fifth of car buyers would most likely need to turn elsewhere in their purchasing decision if the highest level of self-driving technology

needs the collection and sharing of personal data about owners. Our findings suggest many consumers will most likely consider privacy concerns as part of their purchasing decision. The work to date concluded that the collected info could indirectly or directly be utilized to decide the vehicle owners.

Autonomous vehicle (AV) technology is rapidly advancing with vehicles now able to perform most driving tasks while also collecting and storing a large amount of data [6]. Traditional data sharing solutions link multiple data sources sporadically, subject to communication requirements, and equipped with limitations that enable them to share data related only to single or a few types of requests [5]. To support traffic safety and provide efficient traffic management and control, an autonomous vehicle should send messages or share its position and current condition through a V2X system in digitized and timely fashions. Emerging advances in autonomous vehicle technology have tapped the potential of various benefits including emission reduction, less time to follow routes, decrease in road congestion, and the capability of minimizing vehicle accidents. Autonomous vehicles are regarded as a significant aspect of the ongoing revolution in the field of smart cities. In practical environments, crash-related signals from normal vehicles will be detected in advance by your V2X system, alerted on time, and transmitted to cloud servers.

3.1. Ethical and Legal Implications

We integrated two streams of ethical and legal implications of the data privacy challenges: (ELI1) how the existing and potential stakeholders perceive the stronger privacy controls attributed to AV data privacy concerns, and (ELI2) the ethical perspectives and statutory mandates that determine the extent to which the composition of AV data passes through the autonomy transport ecosystem. The four dimensions of the privacy control model presented in this research exercise require a greater influence on the model's stronger existence: scalability, heterogeneity, interoperability, and mobility [6]. Together, the broader set of seven submechanisms of the privacy framework lead us to cover 15 ethical and legal implications. For the practicality of autonomous vehicles (AVs) to emerge from the current experimental settings and transform into a credible social adoption, the two streams of ELIs require meaningful attention toward developing human-centric privacy controls, diligently addressing all the complexities revealed in this research.

While the implementation of privacy controls mitigates the underlying data privacy concerns themselves, on the broader social spectrum traversing different stakeholders, multi-hued ethical and legal implications (ELIs) arise at the crossroads of data privacy challenges, the scale of their privacy controls, the various dimensions of AV data drives, and the varied stakeholders involved. ELIs are sensitive to culture, societal norms, and political regulations [11]. The consumer acceptance of AV technology depends not only on the perceived threat from different ELIs but also on the extent to which these ELIs are satisfied by the autonomous transport ecosystem [9]. A deeper understanding of the ELIs concerning AV data passing through various stakeholders, and addressing them suitably with human-centric privacy controls, will drive the success or failure of AV technology in the competitive marketplace.

3.2. User Perceptions and Attitudes

The gender-based and age-based differences in perceptions are important for developing user-specific privacy controls. As mentioned earlier, many privacy survey items have only been tested with university subjects. The survey used in this study is unique for some important reasons. First, it focused on the adult population to get a better representation of the current legal vehicle users. This study shows that older females are more concerned about sharing driving data with companies. This information will help in the design of user-specific privacy controls. Secondly, it used only car-dependent people, who may be more likely to buy an AV [2]. A recent study conducted by Ipsos and the National Safety Council (NSC) found that only 36% of people feel comfortable with the idea of riding in a self-driving car. Communication about the privacy measures built into AVs may improve perceptions of AVs in general.

Concerns about privacy can impact consumer acceptance of autonomous vehicle (AV) technology [6]. Knowing more about consumers' perceptions of privacy will help AV developers communicate effectively with the consumer population about privacy controls during the adoption phase. Davison et al. surveyed approximately 300 cardependent adults in two rounds. The first round of the survey collected demographic data; previous familiarity with AVs and privacy considerations were ascertained. The second iteration found that 80% of current vehicle users use ride-share services (n=165) were familiar with the term AVs, but only 31% were "very" or "extremely" familiar. Thirty-eight percent were dissatisfied or could not choice. Females are more likely than males to perceive data privacy as a barrier to AV

acceptance, and non-Whites perceive legal liability concerns as a serious impediment to autonomous vehicle use, which female and older populations are more concerned with legal liability issues than male or younger populations [9]. Younger people perceive fewer privacy issues in AVs, but all groups of age are equally familiar with the issue.

4. Importance of Human-Centric Design

It is however, not only important to reduce the amount of personal data collected, but also to ensure that all the other limitations equally respect user autonomy. Just as the spreading of automatic number plate recognition systems may be read as a nudge toward the withdrawal of the cash-based economy, we also envision autonomous vehicles to act as an early and rapid detector for the social sensitivities detected in the earlier space-sharing narratives. We forecast that data-driven practices may inadvertently become a battleground upon which cultural and social norms about mobility, property, and work within the city can be played out. Therefore, opening up a shared autonomous vehicle also becomes akin to opening up the car to any variety of a semipublic context. An autonomous vehicle is configured for a specific context and, without the driver, has a very limited capacity to offer privacy and dignity related to transportation. Like open office layouts and cameras trained on workers, portable data systems are reaping information once shielded. The use of portable data to inform inclination decisions has fostered considerable concern [12]. Thus, the tendency to measure more things is not celebrated in all contexts. We believe that, like the choice of complementary sensor fusion to potentially secure the parking of a vehicle, scoping architectural variables to respect dignity in high-involvement / private contexts is another research question at the intersection of vehicle design and data practices.

An essential theme in all of the articles is how human choices are respected in the final design, and this text revisits the research to indicate the compelling reasons to take a human-centric approach. The three privacy concerns mentioned in [1] highlight the importance of respecting individuals' choices around the use of their personal data, use that is gravely impacted by the forecasted collection of highly personal and commercially valuable data by autonomous vehicles. The scope of the second concern, personal information, gives us an understanding that if we are to collect data to be used by third parties, such as city planners, we at least have to ensure minimal collection of personal data. The final concern, surveillance, can manifest not only when local authorities request data on a specific citizen, but also in the construction

of carbeams aforementioned as they link to and reveal information about individuals. Where we mentioned that there should be minimized collection of personally identifiable data, one should also bear in mind the trend of creating larger datasets by fusing information streams.

4.1. User-Centered Design Principles

Thus, users' privacy and ethical concerns and their values and beliefs are foundational issues in designing privacy controls in autonomous vehicles. In an initial stage of the vehicle design process, we can start identifying scenarios and challenges where privacy controls may be needed in order to secure user privacy and autonomy during driving, whilst not hindering their safety and safety of bystanders of the vehicle. For instances, in a collective philosophy of driving, autonomous vehicles may have to tcehm make collective privacy choices of vehicle owners under certain circumstances, to protect users' privacy, comply with the law, and thereby pursue the collective benefits of the vehicle owners under the constraints of such laws, similar to the collective privacy infringement cases the researchers proposed in their 'mindware-aware' privacy strategies. The decision-making process at the initial stage can take into account the ethical adoption framework in order to ensure the vehicle design and its implementation and use promote those values and beliefs that are dear to the various stakeholders in the driving domain. In the actual design implementation phase, the user-centered design served as a guide for empowering users to make appropriate privacy decisions in the autonomous vehicles, while respecting users' privacy and ethical concerns by integrating the requirements of the privacy by design framework as a part of the proposed strategies in the design of privacy controls for autonomous vehicles.

In this section, we outline the user-centered design principles used in our study. In particular, we will discuss the focus on human values and privacy and ethical concerns in autonomous vehicle data sharing design; attributes of designing with users in a manner that promotes their inclusion; how appropriate user experience with privacy controls can affect their perceptions of privacy risks and intentions to share data; and, their implications for designing privacy controls for autonomous vehicles. These observations are in line with related research highlighting the importance of messaging in privacy controls¯as well as the need for more understandable and actionable measures for novices in a domain of information technology [13]. Most importantly technical literatures have emphasized that ethical standards, privacy by design and human values should be given profound importance in the design and

implementation phases of technology. This can lead to systematically design and develop human-centred and ethical technologies in general, and in autonomous vehicles domain in particular [14].

4.2. Accessibility and Inclusivity

The survey showed that the importance ratings for most AV-PHAs and EB are significantly associated with the importance ratings of general factors, whereas this was not the case for EP. The participants reported an urgent need for privacy controls. For scenarios of data sharing with local government and private entities, there are also demands for by whom, for what purposes, and to what extent the AV data should be shared. When sharing the AV data with family members, the participants mostly agreed that they are willing to share, but they nevertheless request privacy controls in the form of an alert or they want control such that they are informed before the data sharing takes place. A worst-case scenario is when a user (their life) is subjected to danger while riding in an AV, and participants urge that in such situations it should only be allowed to share the AV data with the police and the road operators. The present study showed that the AV user represents a group that cannot be completely included in the current interface designs. It is important to consider the users' knowledge, age, impairments and language, as well as having a comprehensive picture for inclusion.

This research presents user perspectives on privacy concerns and the need for intelligible privacy controls for AV data sharing. Participants' privacy concerns focus on data sharing and their private data being inappropriately used against their interests [12]. The user study explored (dis)preferred situational use of AV location data in cases of interest of third parties (local government and family members) and private entities (insurance and marketing companies). Our findings advocate for flexibility and user control over privacy settings [15]. Participants want to balance the privacy–utility trade-off in more nuanced ways than allowed by binary privacy settings. Our study also found serious accessibility and inclusivity concerns, that can further marginalise already under-represented populations. Notably, these take the shapes of informing users on how to use the technical functions and making the interfaces sufficiently clear, having accessibility settings for special needs groups, and understanding language, relational, age, and literacy disparities [16].

5. Existing Privacy Control Mechanisms

Much of the survey works focusing on the privacy and security issues of the safety implications of connected vehicles. In a survey paper, the known internal and external privacy significantly influence user preference and vehicle functions, and the value remains even under worse conditions, such as nonpersonal data in the network, but overextended lifetime of the users. As one of the first papers, we propose a privacy-related trust concept. We collect and investigate general privacy-related trust tendencies, different models of privacy-related trust in a crowdsourcing scenario, and different privacy-related trust quantifiers in the discussion. We break down privacy-related trust by its impact on different stages of user data collection [3]. This survey aims to create a coherent and solid foundation of the existing state-of-the-art by collecting related work in literature on privacy. Such a survey can be targeted by privacy-enhancing systems of the future connected vehicle ecosystem and by addressing the current operational shortcomings.

Training autonomous vehicles (AVs) usually requires a large amount of training data, including personal information, reputation battlegrounds that can expose the vulnerabilities in the data pipeline, and personal information in the trajectory of the vehicle, and the reputation battleground that can expose the vulnerabilities in the loyalty data pipeline, which make it particularly vulnerable to privacy attacks [7]. Existing privacy protection approaches mainly focus on four aspects: data aggregation, anonymization, data deletion, and homomorphic encryption. However, these approaches are mainly focused on theoretical research and have limitations when conducting large-scale practical applications. For example, data aggregation requires all information to be shared, and then all information is added. It cannot guarantee the control of detailed privacy, and in the real application scenario, it is difficult to be acceptable to the vehicle and the individual.

5.1. Review of Current Solutions

In the context of the connected vehicle, there are numerous other security and privacy concerns referring to individual drivers, ecosystems, and infrastructures. Widespread usage of modern CPVHSS has a significant potential to improve driving and road safety by providing a number of additional features for specific vehicle situations. Nevertheless, this aspect also requires proper consideration and well-balanced reactions from vehicle manufacturers or independent software developers for the ecosystem's threats. Crucial factors

of the successful digital transformation of the automobile industry will be balancing human-driver interaction with intelligent systems and understanding future business models [5].

...

As discussed in Section 2, privacy regulations and directives have been developed by national and regional policymakers and regulatory bodies to govern the use of PII and other personal data by organizations. In the connected car context, these legislations apply to car manufacturers and service providers, who must handle the personal data collected in the vehicles according to the regulations [17]. However, even though drivers are the ultimate owner of the personal data generated by connected cars based on current data protection laws, they do not have complete control over the use of this data and the possibility to hide it from interested parties (e.g., authorities, insurance companies, research organizations) in case of events requiring additional analysis or audit (e.g., road accidents) [6].

5.2. Limitations and Challenges

As the determination of the optimal privacy controls was made through a heuristic and participatory design process, it might not reflect the challenges that could be imposed by longitudinal sharing while considering adaptation of possible future technologies such as differential privacy [5]. Understanding the preferences of car users may also necessitate a better comprehension of the data sharing schemes that consumers will choose at appropriate levels of costs. Last but not least, it is possible that the political climate of the day might have influenced our user sample. We included this note under discussion, as implementing user control in a system often requires not only the designers' but also the users' consent and the regulators' approval.

As we were collecting and processing data in a lab setting with access to a well-informed proxy user and vehicle system expertise, there were limitations on achieving actual driver perspective or a production-level vehicle data sharing interface. Transferability to vehicles with less standardised vehicle network interfaces are also a limitation of the presented system. There are already early signs of more advances in user controls and data handling affairs in the sector where a full control for the users are being considered [18]. Future works around these concerns can encompass how to present as useful and meaningful a scope that is reduced to reflecting rather more opportunities for drivers by considering all the potential

data shares. Considering domain regulations and new updated privacy and data exchange requirements should also be incorporated.

6. Proposed Framework for Human-Centric Privacy Controls

This paper presents a foundational and descriptive framework about Privacy by Design enacted through decision interfaces and privacy controls in the context of autonomous vehicle data collection and sharing. Our aim is to provide guidance for a human-centric approach to the design of data practices in digital systems. A 'human-centric' paradigm shifts the focus of research from system-centric privacy-passive mechanisms to user-centric empirical studies and principled interfaces and controls. We then review data on AV data sharing practices and investigate privacy controls in the context of Personal Data Spaces (PDS) with a particular emphasis on data sharing. We find that while system-centric Passive Mechanisms such as Notice and Consent provide a basic set of controls, they are likely insufficient in an AV context. We propose to integrate insights from empirical human-centric studies into the design of a new generation of Empowerment Mechanisms and Controls in AV data practices, pathways, and interfaces to provide an effective solution to managing privacy [6].

According to Stahl [19], the design phase is the key phase to embed values and principles into AI systems. Privacy obligations are the most important factors on privacy protection and a key challenge is to understand the nature of these obligations to create a responsible approach to the ethical design and deployment of AI systems. As AI systems interact with personal data to gain insights, privacy is the foundation that shapes the sustainable development of AI technology. It is necessary to consider privacy inherent in the design process as a whole, not only during the use phase, in order to address some of the shortfalls of existing approaches in dealing with privacy [7]. Privacy by Design presents a strategy for embedding privacy into systems throughout their design phase. Integral to the concept of Privacy by Design are seven interdependent and mutually supporting Foundational Principles. These Principles guide users to implement the Privacy by Design framework within organizational operations, including technologies, physical architectures, business processes, and practices. The framework presented in this paper assumes that user interaction is the primary mechanism through which privacy risks are managed in digital systems. It will be shown in this paper that Privacy by Design applies from the design of the whole system down to the design of specific privacy decision interfaces.

6.1. Design Principles

Why, What, and When: With reference to the various layers of virtual autonomous drivers, the authors are concerned with explaining the aforementioned principles with the purpose of disclosing the rational behind the rules (w), the various autonomy layer positions on which the directly dependent functions are available (w), the specific distances making these countermeasures taking more or less effective (w), and the operational context special dates inside which the privacy concern is expected to be relieved developing a trade-off between shared and protected information [20].

Assumed Social Distancing: To maintain the social distancing among the users while engaging in data sharing, different strategies are proposed. For instance, it is proposed that no user should be able to get's other user's external data and this could be utilized to avoid the possibility of any kind of online/offline tracking. A derived principle from this human-like privacy feature is, if the user trusts the anonymous and hidden data, he/she should also trust the data produced from following each other, distance of vehicles different. Consequently, in order to have predefined unpredictable behavior in terms of privacy, the assumption of social distancing safety is considered as a design principle [5].

Pareto Superiority: In autonomous vehicle data-sharing, Pareto optimality was identified [article_id] as the most prominent criterion that poses a crucial role in determining the adequate distribution of benefits among the involved stakeholders

[2] With an aim to ensure systematic and controlled considerations for the design of an effective privacy control on authority data sharing, a set of design principles have been described in the following:

6.2. User Interface and Interaction Design

An iterative user-centred design process was used to gain insights about users needs, affordances and preferences, and to make informed decisions about design, without losing sight of usability and privacy considerations. To that aim, the design of the user interface and the interaction model follow a user-centred design approach. We carried out this 'design, evaluate, re-design' cycle based on three studies. Our prototype aims to explore the possibility of achieving a user-control-centred experience while taking into account usability, user preferences and consent, privacy features, ability to comprehend and usability [15].

Privacy-associated data illustrates the manner information can be exposed to unwanted parties. Nowadays, with the increased popularity of autonomous vehicles, there are major concerns involving the collection and sharing of a range of data sets, which raises the necessity to design user-centric privacy controls for sharing autonomous vehicle data. Project results from the paper drives the design of a human-centric system that aims to let drivers have the ability to perceive and to control the necessary data collection while making directly informed decisions about data sharing. Usability and privacy were combined in order to meet user's goals and preferences [17].

7. Case Studies and Implementation Examples

One of the ways in which this challenge has been tackled is through the adoption of a user-oriented design approach, and the resulting provision of means for the user to gain control over the sharing of their data. A study on the attitudes of the public to CAV data sharing showed that the more options offered, the more germs were being shared, but the distorting effect of the menu of a 'large buffet' was found to be limited. This 'buffet-style' offer might be valuable as a means to demonstrate values and intentions over the full variety of types of data that a CAV could be tricked with [18]. This approach was partially based on insights from before, e.g. a review of 20 GDPR notices found that they were usually vague or confusing enough to neglect almost all the rights assigned by the regulation.

CAVs risk up to 25 gigabytes of data per hour for all journeys and use this data not only to provide insights, but also to share data to provide a wider range of services [21]. Sharing CAV data widely or inaccurately could pose privacy and safety risks and CAV developers have engaged in research in this area, for instance, to define new possibilities for the combination of GSR-3 data sharing types, and to explore perceptions and expectations regarding the types of data that are shared [13]. Although, the characteristics of the data that CAVs collect are unlike large numbers of consumer electronic devices that might typically be included in the literature on the sharing of data from smart devices, some findings on data can be mapped straight onto the point on the sharing of data from CAVs that one concern is misalignment or misunderstanding about the purposes of a data-sharing process.

7.1. Real-World Applications

These privacy concerns showed that the ownership aspect has a significant influence on trust and acceptance of the services in AV technology. After a crash, police can access the event data stored in the black box of the vehicle, but depending on the data-gathering period of the data, the user can also access the data and delete it in carmediated communication. Moreover, since the sensitive data are limited to the number of events with high consumption of memory, on request of the owner, the vehicle can download the data to bring them to safety.

! Our narrated video scenario was designed to cover a wide range of situations, [6] including crashes, when privacy was quite sensitive from the user's point of view. In our video scenario we presented a mechanism by which the vehicle directly informs the driver that it noticed a potential crash and asks the driver if they would like to share the vehicle data with emergency services. The user can make the decision after being informed about the consequences of the choices. The users could also enable automatic sharing in the future as part of the 'privacy preference' setting. The study participants found it very useful and natural to be asked if they wanted to share information after a potential crash, and they liked the privacy-by-design strategy that empowers them by including them in the data-sharing decision-making process using a driver-always-in-the-loop approach. As one participant noted, crashing and fatalities could be present in a user's model even against the risk of possible data misuse, and they defined the role of the technology as data security in their sharing process. Nevertheless, participants still had serious concerns about AVs and potential data usage or processing to recognize their fragility about the topic. Indeed, even though it is intended for law enforcement or legal investigations, sharing shared data with legal institutions remained a major concern among end users from the user-to-user interaction, which extended to data privacy management and control with multimedia and context awareness. [12]

7.2. User Feedback and Usability Testing

This was partly in order to help inform our future research but also to provide more widespread information to the public bringing in the privacy risks connected to data sharing and in the future, designing the use of automated vehicles. As it is essential to consider user feedback in the development of new systems for privacy awareness, we have employed an exploratory study, including a survey, to understand user attitudes and knowledge about privacy in the use of the data collected from AV sensors [22]. Research on requirement elicitation includes careful work with the stakeholders from the following disciplines: ethics,

psychology, political science, computer science, information engineering, law and management. We perform user studies aiming at understanding user attitudes to privacy in connected cars in order to facilitate a process of informed consent. User attitudes towards the use of different sensors are also compared. The survey was extended when we discovered that new dimensions were emerging from the community. This study will inform the design of a privacy-by-design approach to the consent mechanism in the autonomous vehicles.

Mature models of human-centric design include the need for user feedback and iterative user testing [23]. This necessitates including potential users in the design process. One of the objectives of this research has been to fill an identified gap in the literature to not only look at user requirements but to also assess content and presentation of these requirements by user tests. Additionally, the measures could be used to assess the success of the system, whether it is meeting user requirements. In order to achieve this, users were required to complete all of the tasks, which mimicked the functionality the application would provide but in a dummy system, to assess the time taken and to measure it without influencing the usability study. Data was also collected on the performance of the users in multimodal interaction in the haptic and voice interaction. Finally, as an exploratory study, participants were given further abilities to make comments or critique the various voice commands, however, this data was not used to shape research in the first instance but was used to highlight those areas the participants found problematic. One of the consequences of these encounters can be to raise awareness of privacy risks related to the use of automated vehicles.

8. Evaluation and Assessment of Privacy Controls

The expectation is that privacy researchers in collaboration with user and vehicle interface experts provide guidance on how privacy and consent management can be effectively communicated and managed in a user-centred, objective-oriented and clear manner. In the automotive sector, particularly in the context of car data sharing, the provision of such user friendly, privacy-secure and fail-safe interface options for objective-oriented control as envisaged in RQ2 is, to our knowledge, new. However, similar notions are already known in the context of human-computer interaction research, e.g. from the Relevance Feedback and Dimensionally-Reduce Data Space user interface paradigms in category learning [6], and in connection with ethical approvals, where participants have to engage with and manage complex consent processes.

A brief review provided by Li et al. [7] suggests the importance of user control in managing privacy in connected and autonomous vehicles. As the car industry is focusing on developing user-centric privacy management tools to gain the trust of future users and preserve the competitive advantage over technology and IT companies dealing with user data. To focus the discussion on research questions R1 and R2, the aim of this section is to provide an in-depth review of privacy-related factors for developing user-friendly interface options and control tools for managing user's consent with the sharing of their car data.

8.1. Metrics and Evaluation Criteria

In [Seg 5], we have discussed the privacy and usability metrics, as well as the scenarios and information necessary for their examination within scenarios about autonomous vehicles. In addition to the relevant technical and usability, factors such as the perceived privacy can show notable variability across different personas, even if they share similar behavioral practices [Riw 12]. Thus, having a perceptual evaluation in place makes it also possible to better take satisfaction and acceptance by users into account, and allow developers proper validation of their solutions when introducing potential improvements on a more realistic basis [Hom 15]. As shown in [Zin 10], such a multidimensional approach can also be considered as being more efficient at revealing insights than a more in-depth elaboration of a single one. For the establishment of consensus across research endeavors and projects towards going beyond traditional, focus-group based evaluations, the provision of the used and recommended methodologies is widely accepted in the value-sensitive design field [DeK 16]. In the context of the self-driving car and by using perceptual evaluation involving diverse stakeholders, [Mar 14] found that the results strongly vary, and demonstrated that older and female participants hold stronger privacy concerns.

8.2. User Studies and Surveys

First, in the project RESOLVE on ABC, a description of the different types of data that attract participants was provided, and participants went on to create a dynamic priority list for the data sharing of an abc-driven AV scenario [24]. Details on this project can be found in the respective case study of this exemplarily special section; furthermore, feasible measures regarding privacy protection for electromobility were also identified. That study was followed by a survey in the project Shared Mobility, investigating not only data sharing with and within a pod-shaped vehicle, but also the wish to disclose data in an urban environment. Even

though the participants of the Shared Mobility study were well aware of the hypothetical scenario, they were still willing to accept churnalistic push news from the AVs, stating preferred content including detour information, weather and traffic conditions as well as news on attractions on interesting topics, e.g., regional history, geology, and nature protection. In study three, based very closely on a case that was developed for the art project NO LIE NO CRY, participants were allowed to touch and smell a tactile installation with lipstick, lacquer and lipstick ingredients [13]. The objective of this project was to investigate the willingness for the determination and sharing of safety-related data with industry and public authorities in the context of autonomous driving.

Data sharing by autonomous vehicles can lead to privacy violations. In order to address this concern, Wistar et al. [5] present, as an example, a prototype of a dynamic privacy control mechanism, which allows the driver to create privacy constraints in the form of wishful data packages covering specific road segments and gets suggested pricing for its sale to an AV-based transportation solution. Put differently, users can decide, which amounts of which type of their personal data are admissible for storage and transmission, and for what reason and how consideration should be provided. However, in order to derive efficient privacy control solutions, the individual privacy preferences must be understood. In this context, engagement and co-creation are of great relevance, and intuition-building collaborative design approaches should be applied. Only then, user-friendly privacy controls can be created. This is why this section presents three studies aiming at the investigation of user preferences, fears, needs, and suggestions regarding data sharing, privacy, and autonomy.

9. Future Directions and Emerging Technologies

Future work in the domain of location-based services, mobility paradigms and business models, and vehicle scenarios should take into consideration the establishment of a multi-methodological approach. Currently, a variety of research methodologies have entered the domain of autonomous systems and LBS, aiming for the advancement of legal out to technical and visionary aspects; however, such research should be still extended further. Additionally, an academic paradigm building should be installed in an effort to bring privacy-oriented discussions among a wider public community. Ultimately, to secure shared data, it is important to consider new standardsization and regulation measures, e.g., electronic data sharing system interoperability, standards for data catalogues pertain LBS driving data, data

sharing system App, and data sharing agreement standards and regulations. Moreover, the consideration of future simulation methods provides a first basis for more sophisticated mathematical and technical aspects in evaluation. Owing to the enhanced ethical impacts of data and privacy, future work could consider an extension of user studies and experimental research in, e.g., driving simulators. For example, researchers can apply methods known from cognitive sciences (learning and memory) to determine memory and retention of privacy deactivating features in experimental settings. Future work could be extended by legal ponders, including, e.g., economic lavishness of privacy, a further ethical research, and advanced representative surveys of societal consent.

[2] [25] [1]The design, development, and deployment of autonomous vehicles are likely to significantly evolve in the near and long-term future, from experimental and test deployments to full commercialization, growing availability and market penetration. These changes will be accompanied by new regulatory requirements and data sharing policies, novel business models, and potentially different architectures and technology standards and protocols. Some directions that have been identified include future work encompassing the establishment of further taxonomies of data, development of ethical frameworks and provision of support and regulations. Other identified research directions in the emerging area of autonomous vehicles and data sharing include (a) the design, development, and deployment of privacy- and data sharing-aware location-based services (LBS), (b) novel mobility paradigms and business models based on LBS usage, (c) novel user contexts, requirements, and feedback in LBS, and (d) novel approaches for privacy management (including open topics in the development of vehicular services and vehicular network architectures).

9.1. Technological Advances in Privacy Protection

A person driving a vehicle is a fully autonomous actor generating a vast variety of passenger-related data. In principle, in a future scenario such data can be reused, shared, sold, or demonetized for user-related digital services such as health, well-being, games or shopping. The data can also be used for intelligent and multi-functional ambient-assisted environments in which the vehicle will be more than just a means of transport with the capability to recognize intentions, patterns of group behaviors or dynamic passenger and group-forming situations, for instance. [18]. In scenarios of privacy suitable services will care about the selective sharing on demand, the privacy convergence between user, infrastructure and

connected environment, the dynamic regulation of privacy and the context-aware shift from public to private and vice versa.

Privacy is not an exotic topic anymore when connected to intelligent transportation. Reliable and user-centric approaches have to be developed and equipped in order to ensure the privacy of the users' data, where and whenever required. There are multiple technological areas in which advances have to be achieved in data privacy, considering the vehicle as a highly mobile, daily-used, and chaotic data hub. [10]. The survey on privacy revealed that it states, privatness includes aspects that relate to the comfort in situations of companionship, which is based on trust and suspected closeness of digital actors. [5]. Apart from traffic safety, comfortable mobility and vehicle use will need to provide data privacy.

9.2. Integration with Smart Cities and IoT

The information about individual trips could be used for various purposes, such as to optimise traffic flow in cities, allocate appropriate energy resources in the grid and to enable new on-demand services. Data generated by connected services, IoT objects and autonomous vehicles could be valuable in designing advertisements for already interested customers or in improving surveillance technologies. Similarly, with the generated data from CAVs, a large privacy risk may be associated [1]. CAVs can generate rich, up-to-date, and high-resolution data describing the environment surroundings and traffic conditions, and remote attackers can exploit the data to blackmail the driver, manipulate the car, disrupt traffic, or paralyse large areas. With the increasing number of drones in intelligent transportation systems tasked with smart city management and coordination, a lack of privacy-preserving mechanisms may hinder faster and efficient operations.

[7] As part of ever-advancing technology scenarios, the future of mobility will necessarily be dominated by connected and autonomous vehicles (CAVs). These vehicles are likely to be an essential part of smart cities and Internet of Things (IoT) ecosystems. In the years leading up to wider CAV deployment, significant effort is required to ensure the introduction of efficient security and privacy controls is factored into the data sharing technology. Data produced by both CAVs will be part of the growing data servers of urban infrastructure to make future decisions [10] and mobility predictions.

10. Conclusion and Recommendations

[1] In summary, the three major privacy concerns are personal autonomy, personal information, and surveillance. These privacy concerns can be mitigated through the advanced technology of Security and Privacy by Design (SPbD) principles. However, finding the balance between Security and Privacy (SP) is not straight forward, as SP can have a trade-off relationship and this is particularly challenging in the context of fully and partially autonomous vehicles. We identify the following ways to mitigate user concerns over privacy, the introduction of product liability laws for SP violations, the standardization of SP technologies for vehicular networks, and government initiatives to safeguard consumer privacy once they are on board. The education of prospective autonomous vehicle owners is also recommended to allow a greater understanding of SP issues and SP technologies in vehicular network for fully and partially autonomous vehicles. The main threats to systems for autonomous vehicles are, remote control attacks, attacks on GPS and V2V security, attacks on communication systems used by autonomous vehicles, data breaches, and Common Vulnerabilities and Exposures (CVE). With these various kinds of potentials threats on each stored data disposal and the privacy of the data have only discussed in detail in this paper. Hence, this article examines the driverless vehicle threats and examines what data privacy threat this propose from a social perspective. The main aim of this paper to develop the Security and Privacy policy for future vehicle development.[26] We administered an online experiment (n = 318) to assess the effectiveness of two forms of privacy controls (permission sharing and data anonymization), and included user attitudes toward their own data sharing and evaluations of perceived risks to privacy to assess their effects on the acceptance of the most effective privacy controls from the experiment. Findings from our study have significant implications for privacy technology design and autonomous vehicle data sharing acceptance research. We find that the way in which a technology is designed to exercise control over an individual's own data sharing is effective at reducing users' privacy concerns. If non-expert users feel that they are in control of their data, then the potential negative effects of poorly implemented permission requests will be mitigated. Conversely, if expert users feel that they are not in control of their data, then the potential positive effects of well implemented anonymization will be mitigated. Both the development and deployment of privacy controls in autonomous vehicle systems should be handled with careful consideration and attention to end users' expertise, attitudes, and beliefs. Specifically, users care about their own privacy more than the privacy of strangers.

10.1. Summary of Key Findings

Even with two control levels embedded in the challenge-response protocol and both control level traffic observation driver's identity in o N public link in New England, the surprising thing is that over 35% AVs can still be identified unique supporter before the schedule service. On the other hand, when the traffic and service provider need the real name of the traffic provider for identity verification, it can randomly prove the identity to the other views while preserving the real name perceived by the service provider, thus reaching a compromise between privacy and real-name authentication. In addition, they conclude that it is not possible to achieve only platform-side audit A non-embarrassing probability of successful privacy burglars in control.

Privacy has been a significant concern in the context of connected vehicles, for example, the design of privacy protection based on heterogeneous networks for connected traffic environments was modeled in which the user central privacy security with different privacy design was shared and the user private penetration rate was reinforced. However, connected driving privacy involves more than just protecting location data, license plates and trajectories. Curran et al. discuss the privacy of autonomous vehicle (AV) characterization data. These data can be shared to improve the safety and feasibility of AVs but may contain privacy-sensitive personal information. The data subjects may not want their personally identifiable information (PII) to be H. Wang et al. used the simple side of C for pseudo-anonymously obfuscating the serial number of the E except the star character while preserving the random walking characteristic of the serial number ringing. Kirchsteiger et al. proposed an AV data sharing system in which the data is optionally shared with other AVs if the response is non-embarrassing probability of privacy breach.

[2], [27]

10.2. Implications for Policy and Practice

The intersection of data protection and the right to privacy, as stated by different legal approaches, underpins the policy and institutional influences on privacy. Innovations and advancements in technology are affecting ways of handling individual information. There are urgent demands to manage personal information in a more transparent, inclusive, and democratic direction. Further, we noted the importance of uncertainty or non-knowledge to

explain privacy behavior and how its datafication in connected societies, in the form of invasive surveillance practices like micro-targeting, much-promoted personalization or profiling. Technological limitations to privacy are also noticeable and recent advancements in techniques are able to eclipse advantages. Nevertheless, technology could also be the root of solutions. Technological solutions are recognized as key factors for managing our privacy and should be managed to ensure that privacy expectations are suitably understandable for an uncertain society/surveillance studies or a techno-society. [28]

Looking at potential implications of our findings for policy and practice, we note particular institutional and cultural dimensions that form important backdrops. Since the concept of privacy and motivations for it differ in various legal systems, informed by different guarantees and their amendments, different legal systems have diverging regulations. For instance, in the Unite States, the Fourth Amendment to the US Constitution is very attentive to physical space privacy or secrecy. Another example is that regional or federal legal systems in some countries prioritize protecting the personality right over all personal data protection, whereas some concentrate more on the value of the data itself. The interpretation of privacy can also vary according to the cultures of people and countries. [29]

Reference:

1. Tatineni, Sumanth, and Anirudh Mustyala. "Advanced AI Techniques for Real-Time Anomaly Detection and Incident Response in DevOps Environments: Ensuring Robust Security and Compliance." *Journal of Computational Intelligence and Robotics* 2.1 (2022): 88-121.
2. Biswas, A., and W. Talukdar. "Robustness of Structured Data Extraction from In-Plane Rotated Documents Using Multi-Modal Large Language Models (LLM)". *Journal of Artificial Intelligence Research*, vol. 4, no. 1, Mar. 2024, pp. 176-95, https://thesciencebrigade.com/JAIR/article/view/219.
3. Bojja, Giridhar Reddy, Jun Liu, and Loknath Sai Ambati. "Health Information systems capabilities and Hospital performance-An SEM analysis." *AMCIS*. 2021.
4. Vemoori, Vamsi. "Evolutionary Landscape of Battery Technology and its Impact on Smart Traffic Management Systems for Electric Vehicles in Urban Environments: A Critical Analysis." *Advances in Deep Learning Techniques* 1.1 (2021): 23-57.

5. Jeyaraman, Jawaharbabu, and Muthukrishnan Muthusubramanian. "Data Engineering Evolution: Embracing Cloud Computing, Machine Learning, and AI Technologies." *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)* 1.1 (2023): 85-89.
6. Shahane, Vishal. "Serverless Computing in Cloud Environments: Architectural Patterns, Performance Optimization Strategies, and Deployment Best Practices." *Journal of AI-Assisted Scientific Discovery* 2.1 (2022): 23-43.
7. Devan, Munivel, Ravish Tillu, and Lavanya Shanmugam. "Personalized Financial Recommendations: Real-Time AI-ML Analytics in Wealth Management." *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*2.3 (2023): 547-559.
8. Sharma, Kapil Kumar, Manish Tomar, and Anish Tadimarri. "Optimizing sales funnel efficiency: Deep learning techniques for lead scoring." *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)* 2.2 (2023): 261-274.
9. Abouelyazid, Mahmoud. "Adversarial Deep Reinforcement Learning to Mitigate Sensor and Communication Attacks for Secure Swarm Robotics." *Journal of Intelligent Connectivity and Emerging Technologies* 8.3 (2023): 94-112.
10. Prabhod, Kummaragunta Joel. "Leveraging Generative AI and Foundation Models for Personalized Healthcare: Predictive Analytics and Custom Treatment Plans Using Deep Learning Algorithms." Journal of AI in Healthcare and Medicine 4.1 (2024): 1-23.
11. Tatineni, Sumanth. "Applying DevOps Practices for Quality and Reliability Improvement in Cloud-Based Systems." *Technix international journal for engineering research (TIJER)*10.11 (2023): 374-380.
12. Althati, Chandrashekar, Manish Tomar, and Jesu Narkarunai Arasu Malaiyappan. "Scalable Machine Learning Solutions for Heterogeneous Data in Distributed Data Platform." *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023* 4.1 (2024): 299-309.