Understand Users' Privacy Perception and Decision of V2X Communication in Connected Autonomous Vehicles

Zekun Cai and Aiping Xiong, *The Pennsylvania State University*

https://www.usenix.org/conference/usenixsecurity23/presentation/cai-zekun

This paper is included in the Proceedings of the 32nd USENIX Security Symposium.

August 9–11, 2023 • Anaheim, CA, USA

978-1-939133-37-3

Open access to the Proceedings of the 32nd USENIX Security Symposium is sponsored by USENIX.

Understand Users' Privacy Perception and Decision of V2X Communication in Connected Autonomous Vehicles

Zekun Cai
The Pennsylvania State University
zuc204@psu.edu

Aiping Xiong
The Pennsylvania State University
axx29@psu.edu

Abstract

Connected autonomous vehicles (CAVs) offer opportunities to improve road safety and enhance traffic efficiency. Vehicle-to-everything (V2X) communication allows CAVs to communicate with any entity that may affect, or may be affected by, the vehicles. The implementation of V2X in CAVs is inseparable from sharing and receiving a wide variety of data. Nevertheless, the public is not necessarily aware of such ubiquitous data exchange or does not understand their implications. We conducted an online study ($N = 595$) examining drivers' privacy perceptions and decisions of four V2X application scenarios. Participants perceived more benefits but fewer risks of data sharing in the V2X scenarios where data collection is critical for driving than otherwise. They also showed more willingness to share data in those scenarios. In addition, we found that participants' awareness of privacy risks (priming) and their experience on driving assistance and connectivity functions impacted their data-sharing decisions. Qualitative data confirmed that benefits, especially safety, come first, indicating a privacy-safety tradeoff. Moreover, factors such as misconceptions and novel expectations about CAV data collection and use moderated participants' privacy decisions. We discuss implications of the obtained results to inform CAV privacy design and development.

1 Introduction

The U.S. road transportation infrastructures are verging on the most significant technological transformation since the introduction of the automobile on the road. To facilitate the operation of connected, autonomous, and connected and autonomous vehicles (CAVs), the existing infrastructures that ensure mobility are being replaced with intelligent transportation systems (ITS [92]). Leveraging the vehicle-to-everything (V2X) communication [75], the ITS enables the exchange of driving relevant information between a vehicle and any entity that may affect, or may be affected by, the vehicle, supporting interconnected vehicles' operations to be performed autonomously [52].

While deploying the ITS and V2X communication is promising to have enormous social and technical benefits (e.g., enhancing road safety and improving traffic efficiency), they also offer the chances for privacy and security attacks [72, 82]. In particular, drivers and passengers of CAVs are required to share heterogeneous data (e.g., vehicle identity, speed, and GPS coordinates) at unprecedented speed and scale, exposing them to potentially severe privacy invasions.

Prior studies have explored users' perception of CAVs [12, 16, 17, 20, 93] with a focus on *vehicle-based* sensing and recording (e.g., data collected by external camera, radar, and LiDAR). Those results generally show that participants underestimated the capability of vehicle-based data collection and their secondary use (e.g., identification and tracking). Participants' perceived benefits of such data collection (e.g., enhancing driving safety) were context-dependent (e.g., interacting with the vehicle as drivers or bystanders [93]) or varied among individuals (e.g., prior experience with driving assistant systems [17, 20]). While those efforts provide an initial understanding of *human aspects of privacy* for CAVs, they have mainly focused on vehicle-based sensing and recording. It is not yet well understood regarding the privacy of CAVs from the *connectivity* aspect (i.e., V2X communication).

Previous research on V2X communication privacy has focused on technical aspects and proposed anonymization [6, 81, 87, 105], perturbation [3, 98], and differential privacy (DP [5]) methods to protect identity privacy and location privacy. Little work has addressed the issue by considering the *user* as an integral privacy component. However, due to lack of knowledge about and experience in emerging CAV technologies, users' privacy awareness of V2X communication might be low and consequent privacy control might be limited [55]. Moreover, the data collection and analysis of V2X communication are diverse and dynamic [72]. For example, different types of V2X communication (e.g., vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) [32]) have been applied to various application categories (e.g., road safety and traffic management [30]), raising novel challenges for users' adequate privacy awareness and informed privacy decisions [71].

In this work, we fill the gap toward understanding users' privacy perception and decision of V2X communication in CAVs. We examine whether, how and why users' privacy perceptions and decisions vary among different V2X application categories. To inform the design of privacy risk communication in CAVs, we also investigate whether priming would change users' privacy perceptions and decisions. Moreover, we explore whether users' prior experience in connectivity and driving assistance functions would have any influences.

We conducted an online experiment ($N = 595$) on Amazon Mechanical Turk (MTurk) using a mixed design. There were three between-subjects conditions: *control*, *privacy priming*, *privacy&security priming*. Participants were informed of potential privacy risks of data disclosure in the privacy-priming condition. Security risks of receiving data were further shown in the privacy&security-priming condition. The four V2X communication applications were within-subjects: 1) *cooperative autonomous driving*, 2) *road safety*, 3) *traffic management*, and 4) *infotainment, comfort and convenience* [30]. During the study, participants viewed one scenario describing the data exchange and its purpose of each application. For each scenario, participants indicated their 1) perceived benefits, 2) perceived risks, 3) data-sharing decision, and 4) data-sharing decision confidence. We also asked an open-ended question at the end to understand why participants chose to share or not share their data in each scenario.

We obtained several important findings. First, participants perceived more benefits but fewer risks in the three scenarios where data sharing is critical to driving than otherwise. Their privacy decisions were aligned with such privacy perceptions (Sections 4.1 & 4.2). Response to the open-end questions confirmed that participants believed that *safety comes first*, indicating the critical role of *privacy-safety tradeoff* (Section 4.5). Second, the privacy priming was effective in encouraging safer data-sharing decisions in general. Yet, the extra security priming did not increase the priming effect (Sections 4.1 & 4.2). Moreover, participants' prior experience in connectivity and driving assistance functions impacted perceived benefits and risks of data sharing, as well as privacy decisions (Section 4.3). In summary, the contributions of our work include:

- We conduct an online study investigating users' privacy perception and decision of V2X communication for CAVs as a result of considering benefits and privacy risks of sharing data, and benefits and security risks of receiving data.
- Besides privacy-utility tradeoff, our results suggest the critical role of privacy-safety tradeoff in users' data-sharing decisions of V2X communication in CAVs.
- We identify various factors (e.g., safety, privacy priming, and prior experience) that can influence people's perceived benefits, privacy risks, and data-sharing decisions of V2X communication in CAVs.

2 Background and Research Questions

In this section, we first describe vehicle-to-everything (V2X) communication in CAVs, focusing on the communication types and the main applications. We then discuss privacy challenges of CAVs, previous research efforts examining people's privacy perception and decision for CAVs, the effect of driving technology experience on people's perceived risks of CAVs. We summarize our research questions (**RQ**s) at the end. We notice the extended length of this section, which is justified given the novelty of research topic.

2.1 V2X Communication in CAVs

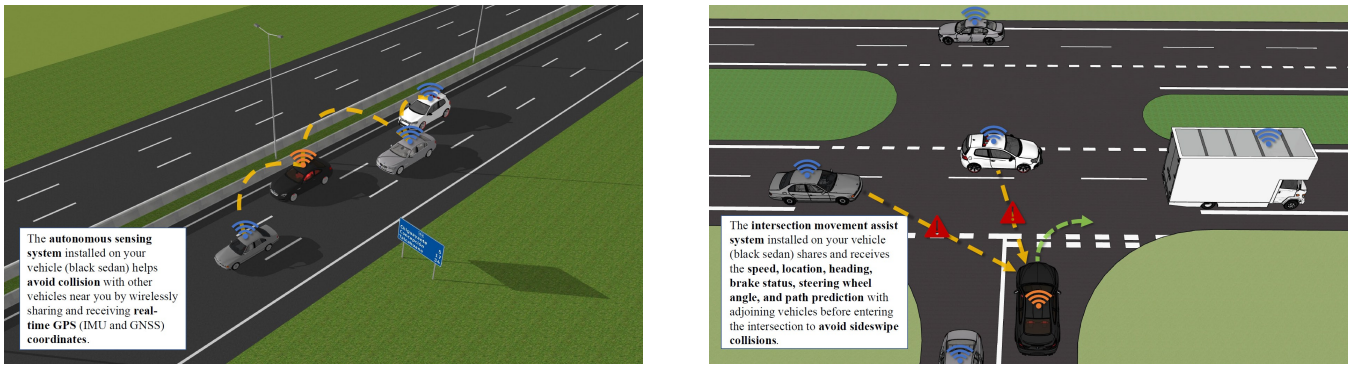
While the data collection and processing by sensors are necessary for CAV functions and features, the pervasive connection with other parties, such as other vehicles and the infrastructure, are critical to fulfilling the promise for CAVs [52]. V2X communication is a wireless ad-hoc technology aimed at enabling data exchange between a vehicle and its surroundings [75].

V2X incorporates specific types of communication such as V2I (vehicle-to-infrastructure), V2V (vehicle-to-vehicle), and V2P (vehicle-to-pedestrian). Take the V2V communication as an example. When a CAV brakes suddenly, it can transmit a notice to vehicles behind that enables those vehicles to warn their drivers to stop or automatically apply brakes if a crash is imminent. Generally, V2X applications in CAVs can be separated into the four categories [30]: 1) cooperative autonomous driving, 2) road safety, 3) traffic management, and 4) infotainment, comfort and convenience (see Figure 1).

Cooperative Autonomous Driving. Self-driving applications mainly rely on sensors inside and outside the vehicles (e.g., LiDAR and radar) to achieve automobile recognition as well as other driving roles [7]. For instance, ultrasonic sensors are used to detect obstructions (e.g., animals) for automatic braking. Yet, the limited perception range of those onboard sensors only allows for detecting adjacent vehicles. These limitations can be overcome by V2X communication, which enables cooperative sensing and maneuvering [52]. Through the mutual exchange of sensed data, cooperative sensing increases the sensing range. Cooperative maneuvering allows the vehicles to cooperate efficiently and perform maneuvers with a high complexity based on a common centralized or decentralized decision-making strategy.

Road Safety. To enhance road safety (i.e., the safety of drivers, passengers, and people on the road), vehicle speed control, accidents, alerts, and all sorts of emergencies (e.g., collision warning) on the road can be communicated through enabling the communication of signals and messages of all interconnected entities in ITS [65].

Traffic Management. Data collection and use in the traffic management applications are to provide detailed information concerning cars, drivers, and status on the roads, which are expected to enhance traffic flow control and synchronization



(a) Cooperative Autonomous Driving

(b) Road Safety

(c) Traffic Management

(d) Infotainment, Comfort and Convenience

Figure 1: Illustration of an example scenario for the four V2X communication application categories. The illustrations are only for concept explanation but not presented in our study.

[89]. For example, these applications will collect and analyze the messages exchanged by ITS entities and communicate existing congested zones to CAV users. Traffic data (e.g., crossing pedestrians) can also be obtained by the deployed road side units (RSUs) and the road sensors to prevent accidents from occurring.

Infotainment, Comfort and Convenience. Data collection and use in these applications aim to enhance user experience in the driving cockpit through services that meet their needs [27]. For example, connectivity to the Internet is expected to be offered to provide access to services, such as online music and videos. Such applications are close to the applications in most mobile devices, which also include weather services, navigation, and entertainment.

How the data are being used in CAVs can be presented in more granular levels [e.g., at the levels of RSU and onboard unit (OBU)]. Considering those unique characteristics of V2X communication, we choose the above coarse, application-level categorization to help us identify major, novel usable privacy challenges, which we apply in the following scenario design.

2.2 Privacy Challenges of CAVs

The heterogeneous data exchanges in the V2X communication could potentially invade the privacy of CAV drivers and passengers in an unprecedented manner. For example, identity and location information broadcasted in beacon messages [61] or basic safety messages [70] can reveal information (e.g., home address) and behavior (e.g., whereabouts) of drivers and passengers. Such information could be linked and exploited for further behavior mining (e.g., home address + whereabouts $\rightarrow$ political ideology). In this work, we examine data exchanges in the four V2X communication applications.

Driving is a highly *cooperative* context [46, 51], in which behaviors such as slowing down to allow another vehicle to merge into the current lane, are expected to communicate drivers' status and intentions [77]. In privacy-sensitive scenarios, individuals' information disclosure decisions can also be impacted by social preferences or norms, such as altruism [2]. V2X communication in the CAVs relies on both *data sharing* and *data receiving*. To comprehensively understand CAV users' data-sharing behavior, it will be critical to understand the potential impacts of data receiving.

2.3 Human Privacy Behavior

Despite the privacy challenges of V2X communication applications in CAVs, little research has been conducted on understanding users' privacy behavior. Using the human information-processing approach [104] we characterize that

individuals process privacy via stages of *privacy perception*, *privacy motivation*, and *privacy decisions*. For each stage, we first introduce human factors that have been identified influencing the privacy in the general online environment [85, 94] and the IoT setting [36, 56, 76], and discuss factors in recording and sensing for connected and self-driving vehicles [12, 93].

Privacy Perception. Privacy perception refers to people's representation and comprehension of possible risks throughout the interaction with an application or service that can gather and process personal data or information [83]. Besides passively receiving information from the environment, human perception is often shaped by individuals' memory, expectations, and attentions [43]. For example, people tend to pay more attention to information that is consistent with their prior knowledge or meet their expectations, resulting in disregarding some information in decision making [13].

In the IoT setting, studies have revealed that users' expectations and concerns about privacy are also shaped by their *prior experiences* with computing technologies (e.g., causing them not to expect privacy by default [97]). Such expectations can also pose consequences to users' privacy evaluations for CAVs, given that over 80% of the U.S. population have somewhat experience with technologies inside the vehicles [88]. Previous studies also show that users' familiarity and experience with driving assistance systems could modulate their privacy perception [17, 66, 100]. A recent online survey examined participants' privacy awareness and decisions on different CAV scenarios using sensor data [20]. The authors found that participants' prior experience with advanced driving assistance systems (e.g., adaptive cruise control) and connectivity functions had a positive effect on their data-sharing decisions. We explored the impact of this factor on privacy perception of V2X communication for CAVs.

Privacy Motivation. Individuals are motivated to share information online by various goals, such as economic benefits [48] and social benefits [22]. While the utility of those disclosure decisions (e.g., low price and social engagements) are typically immediate or instant, possible information leakage or privacy risks tend to be delayed or occur in the future. Prior work showed that users chose low instant reward, which might result in a long-term negative influence [2]. Compared to the general online environment, there are novel motives for individuals to share information in V2X communication, such as road safety and traffic management. Also, autonomous driving and safety could become users' primary motives for data disclosure (e.g., concerns about fatal CAV accidents due to not sharing some diagnostic data). While the safety issues might be distal, people probably choose to share the data anyway due to the severe consequences of not sharing. Thus, existing tradeoff between privacy and utility becomes *tradeoffs* of *privacy-safety* and *privacy-utility* in the CAV context. To the best of our knowledge, this phenomenon is not very understood yet, and our study aims to fill the gap.

Privacy Decisions. Even if individuals can attend to all available information, their ability to translate the information into informed decisions is limited by *bounded rationality* [91]. In other words, individuals reveal systematic biases that deviate the choices they make from the optimal choices assumed rational. The privacy literature has identified numerous cognitive and behavioral factors that affect and sometimes impede privacy decision making [1]. For example, individuals' privacy decision making relies on the first available information (i.e., anchoring [23]), in the default privacy settings [8], or how the information is framed [25, 28, 84].

Priming refers to the phenomenon that when a stimulus (e.g., one word or a picture) makes associated information from humans' long-term memory (e.g., a concept) more available to their short-term memory [99]. Thus, humans tend to consider that information into their consequent behavioral responses. Previous studies showed that participants could be primed by thinking about their safety and privacy through answering privacy statements [49, 84] or viewing descriptions or videos [29]. Thus, regardless of the priming formats (self-relevant questions or factual information), the concept of "privacy" introduced by priming could be activated as part of the task set, which could change consequent privacy behavior (i.e., increased privacy awareness and conservative privacy decisions). We examine the effect of priming to inform the design of privacy risk communication in CAVs.

Vignette-based (or scenario-based) online surveys [38] have been found to well approximate real-world behaviors [47]. Hypothetical data collection scenarios have been used to examine people's disclosure decisions in the IoT setting [67] and vehicle-based sensing and recording [93]. Similar methodologies have also been adopted in the CAV context. Howard and Dai [53] examined participants' attitudes toward self-driving cars and found that the participants were most attracted to potential safety benefits and the convenience. A recent study investigated the CAV service for the purposes of safety/security and convenience [20]. For each service purpose, different CAV scenarios were generated based on varying what was collected. The participants revealed more intentions to share personal information for the safety/security scenarios than for the convenience scenarios. Due to the lack of operational environment for the V2X communication for CAVs, we adopt the scenario-based method in our study.

2.4 Research Questions

The data exchange with other vehicles, infrastructures, and service providers, can make CAVs more vulnerable to data exploitation and cyber attacks than conventional automobiles [71]. Thus, a lack of awareness of V2X communication could result in users' underestimation of the CAVs' privacy risks and uninformed privacy decisions. To understand users' privacy perception and decision of V2X communication in CAVs, we ask the following **RQs** in this work:

- **RQ1**: Given an adequate understanding of CAVs and V2X communication, do participants vary their perceived benefits and risks, data-sharing decisions and confidence across different V2X communication applications? What are the reasons behind their willingness or unwillingness to share the data?
- **RQ2**: Do participants augment their privacy perceptions and decisions of V2X communication if they are primed by privacy&security than participants who are primed by privacy only?
- **RQ3**: Do participants' prior experience in connectivity and driving assistance functions have impact on their privacy perceptions and decisions across different V2X application scenarios?

3 Method

We conducted a scenario-based online survey using Qualtrics. There were three between-subject conditions: *control*, *privacy priming*, and *privacy&security priming*. We created a set of data collection and use scenarios related to the four V2X applications in CAVs (see Table 1). Each scenario described the data flow and information usage of a specific V2X application (e.g., road safety). After viewing each scenario, participants were prompted for different questions. To increase participants' privacy awareness, we presented extra descriptions about the privacy risks of *data sharing* for V2X communication in the privacy-priming condition. Moreover, participants in the privacy&security priming condition were further informed of the security risks of *data receiving*. In the end, participants answered a few post-session questions, including their general privacy attitudes and demographics.

3.1 Constructing Descriptions and Scenarios

The study was performed with participants' own laptops or computers. To ensure the readability of the survey contents, we did not allow participants to continue the study if they were using any mobile devices with an embedded function in Qualtrics [106].

CAV and V2X Descriptions. To situate participants into the hypothetical scenarios for the V2X applications in CAVs, we presented a brief description of CAVs and V2X communication at the beginning of the study, respectively. We also gave examples of the CAV features and different types of V2X communication, including vehicle-to-infrastructure (V2I), vehicle-to-vehicle (V2V), and vehicle-to-pedestrian (V2P). See details of our survey protocol in supplementary material [21].

Comprehension-check Questions. Previous studies have shown that a basic understanding of the survey topic is critical to differentiate legitimate and fraudulent respondents [107]. Participants' comprehension of CAVs could also have impact on their privacy decision-making of CAVs, since the public is unfamiliar with CAVs and related concepts [54]. We applied comprehension check for both CAV and V2X applications. Following each description, we proposed comprehension questions evaluating participants' grasp of each concept. We measured participants' understanding of CAVs by asking 1) the role of human driver; 2) CAVs' data collection and use; and 3) the CAVs' definition. Participants' comprehension of V2X was evaluated through information sharing and receiving in V2I, V2V and V2P, respectively. All questions were True/False questions except that the last question about V2X was a multi-choice selection question (see supplementary material [21]).

Table 1: Proposed Scenarios in Each Application Based on Current Available Algorithms and Techniques

Application	Scenario	Reference
Infotainment, comfort, convenience	- in-car gaming - car parking - in-car video streaming - trip planning	[9], [30], [42], [95]
Traffic management	- location and upcoming trip details - vehicle information - location and speed - speed, heading, and vehicle type	[24], [73], [102]
Road safety	- autonomous sensing - intersection movement assistant - traffic navigation - in vehicle safety and emergency monitoring	[62], [73], [90], [101]
Autonomous driving applications	- GPS coordinates - pictures of surroundings - approaching vehicles, pedestrians, and objects - vehicle movement of the environment	[19], [39]

Scenario Design. We proposed four representative scenarios for each V2X application category based on the literature (see Table 1). Scenarios in each category were concerned with different realistic examples to ensure the representativeness but were nonetheless similar in nature. We specified the purpose of the data collection in a service-oriented manner, so that the daily drivers could better understand the connection of the scenarios to their lives. We also ensured that the scenarios in each category embedded comparable types of data collected and purposes. Specifically, all scenarios included both aspects of *data sharing* and *data receiving*. Thus, each scenario embedded possible privacy concerns and security risks in the data exchange process. We highlighted the key factors in each scenario, such as the application system, data type and collection purpose, to help participants better capture the critical information flow [78] (see examples in Figure 1).

All proposed scenarios were reviewed by two outside experts, one in the field of computer vision and the other in data privacy. Each of them decided individually the validity of each scenario based on a 7-point scale ("1" meaning "very invalid" and "7" meaning "very valid"). They were instructed to make intuitive decisions based on their knowledge and expertise, rather than referring to literature or other materials. Each expert gave an overall rating of 5.7 and 6.1, respectively. The

average ratio of agreement (valid vs. invalid) was 1.0. Both experts rated two scenarios (i.e., online shopping and gaming) in the infotainment category as invalid. Consequently, we deleted the online shopping scenario. Based on the suggestion of one expert, we separated the online gaming scenario into one game scenario and one in-car video streaming scenario. See the finalized 16 scenarios (S) at Appendix A.1.

Priming Descriptions. To shed light on interventions in facilitating private behavior in CAVs, we propose objective, textual descriptions of privacy and security risks of V2X communication. The textual description describes the potential privacy risks of sharing data to use V2X services, which we expect to play a role in privacy priming. Moreover, an extra description specifies the potential security risks of receiving data from external entities, which is expected to have a stronger priming effect (See supplementary material [21]).

3.2 Procedure

Participants were randomly assigned to one of the three conditions after informed consent. There were three phases in each condition. At *Phase 1*, participants read the descriptions of CAVs and V2X at first. Then they answered several comprehension questions to test their understanding of each concept (see supplementary material [21]). Participants in the privacy-priming condition also viewed a paragraph that describes the potential privacy risks of *sharing* data to use V2X services. Moreover, participants in the privacy&security-priming condition received a description that warned them of the potential security risks of *receiving* data from external entities.

At *Phase 2*, one of the four scenarios in each category was randomly selected and presented to the participants. Thus, in this and later sections we use "scenario" and "V2X application category" interchangeably. For each scenario, participants were asked about their agreement on whether they found the data-sharing beneficial and whether they have privacy concerns about sharing the data using a 7-point Likert scale, respectively. Participants in the privacy&security-priming condition also answered two similar questions about their perceived benefits and security concerns of receiving data from external entities. Then participants in all conditions indicated their willingness to use the service by sharing their data, and their confidence in making such a decision. The reasons why they were willing or unwilling to share the data were collected through an open-ended question. The four scenarios were presented in a randomized order.

After answering questions for all scenarios, *Phase 3* started. We asked about participants' demographics (e.g., age, gender and race), their prior experience in using driving assistance functions and connectivity functions in the vehicles, and their overall trust in V2X technology. Finally, we measured their general privacy concern with a subset of Internet users' information privacy concerns (IUIPC) questions [74]. We measured it at the end to avoid any possible priming effect [84].

3.3 Interview Study

To validate the proposed scenarios, comprehension questions, and the survey in general, we did an interview study with six participants (4 females) before the online survey. Participants were recruited using the snowball methods [44]. Specifically, we first recruited participants from our social networks and then asked them to recommend other participants. We requested all participants have a driving license to ensure the sample is similar to the main survey. The interviews were conducted online using Zoom. Besides answering all survey questions, participants were asked to think aloud whether they understood the survey instructions, proposed scenarios, survey questions, and listed options. The interview took about one hour. Each participant was compensated $20.

We gained two main insights from the participants' to improve the survey. On the one hand, participants described that it was hard for them to understand the advanced technologies applied in CAVs and memorize all acronyms (e.g., V2V and V2X). Given V2X and CAVs are still under development, we believe those participants may represent people who are non-tech savvy or have limited experience in using advanced driving assistance or connectivity functions. Thus, we spelled out the acronyms to facilitate participants' comprehension in the online survey. On the other hand, participants found some comprehension questions were hard to answer, such as Q2 in the CAV description and Q2-Q4 in the V2X description. They indicated that there were ambiguities in the relevant descriptions. For example, they failed to capture that each category in V2X communication implies bidirectional communication between the CAV and other parties (e.g., other vehicles, infrastructure and pedestrians) when reading the description. Thus, we highlighted those keywords within the descriptions to increase participants' awareness of the key information.

3.4 Recruitment and Ethics

Power analysis using G*Power 3.1 [37] suggested 606 participants to detect a small effect size (Cohen's $f = 0.10$) of a two-way interaction of 4 (*V2X communication scenario*: infotainment, road safety, traffic management, autonomous driving) $\times$ 3 (*condition*: control, privacy priming, privacy&security priming) with a power of 0.8 [mixed analysis of variance (ANOVA) test ($\alpha = .05$)]. Considering the uncontrolled online setting, we doubled the sample size and recruited 1204 participants initially to ensure sufficient power.

Participants were recruited on Amazon Mechanical Turk (MTurk). The human intelligent task (HIT) was posted with restrictions to workers who (1) are at least 18 years old; (2) completed more than 100 HITs and with a HIT approval rate of at least 95%; (3) are located in the U.S.; and (4) are vehicle owners. Considering the emergent issue of data quality on Amazon MTurk [60] and the public is unfamiliar with CAV and related concepts, we applied comprehension-check ques-

tions to ensure data quality and participants' privacy perceptions and decisions were based on an adequate understanding of CAV and V2X communication (see details in Section 3.1). Based on the interview results, we set a criterion of 5 out 7 to filter out inattentive or fraudulent participants. Among the 1204 participants recruited, 56.4% (680) of them passed the test and completed the survey. We viewed the comprehension-check questions as a proxy for attention check, of which the pass rate on MTurk is about 60% or less [60]. The median completion time was about 15 min. We paid each participant $1.90[1]. Participants who failed the comprehension check (median completion time = 2.3 min) were compensated for $0.50. This experiment complied with the American Psychological Association Code of Ethics and was approved by the Institutional Review Board at the authors' institution. Informed consent was obtained from each participant.

Table 2: Demographics of Participants in the Online Survey

Item	Option	Percentage
Gender	Male	50.6%
	Female	48.7%
	Non-binary / third gender	0.5%
	Prefer Not To Answer	0.2%
Age	18-24	2.7%
	25-34	27.2%
	35-44	25.9%
	45-54	22.2%
	55-64	13.8%
	$\geq$ 65	8.1%
	Prefer Not To Answer	0.2%
Ethnicity	African / African American	5.2%
	American Indian / Alaska Native	0.7%
	Asian	4.7%
	Caucasian	83.2%
	Hispanic / Latino	3.9%
	Native Hawaii / Pacific Islander	0%
	More than one race	1.7%
	Prefer Not To Answer	0.7%
Years of Driving	< 2 years	0.3%
	2 - 5 years	5.7%
	5 - 10 years	11.4%
	> 10 years	82.5%
	Prefer Not To Answer	0%
Mileage (Miles/Year)	< 2,000	6.7%
	2,000 - 5,000	18.5%
	5,000 - 10,000	38.3%
	10,000 - 20,000	27.9%
	> 20,000	8.2%
	Prefer Not To Answer	0.3%

4 Results

Another 15 participants who spent less than 5 min (the shortest completion time in the pilot survey) or longer than 1 hr (the long tail of the right-skewed completion time distribution) on the survey were removed from the analysis. An extra 12 participants who chose "prefer not to answer" in at least one question at Phases 2 and 3 were excluded from data analysis. We excluded another 58 participants' results because they failed to give at least two meaningful answers to the four open-ended questions (manually verified by the authors). For the remaining 595 participants[2], there was an approximately equal number in each condition, control (220), privacy priming (202), and privacy&security priming (173). A similar number of participants was assigned in each scenario: infotainment (S01-S04: 156, 155, 138, 146), traffic management (S05-S08: 164, 140, 155, 136), road safety (S09-S12: 144, 144, 151, 156), and autonomous driving (S13-S16: 135, 168, 144, 148). Table 2 shows participants' demographics.

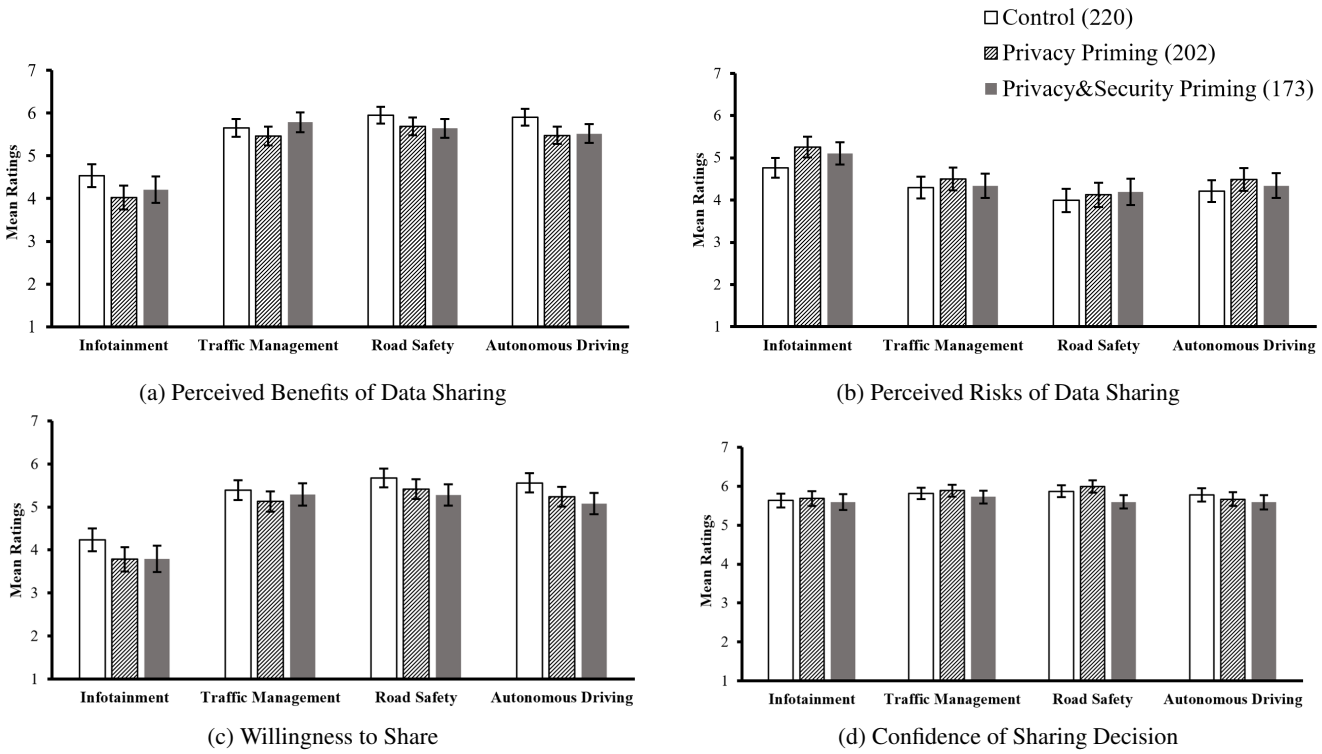
Analysis Plan. Our statistical analysis focused on four measures (perceived benefits, perceived risks, willingness to share, and confidence of sharing decision) related to CAV privacy decision-making at Phase 2. We manipulated two factors: *condition* (control, privacy priming, privacy&security priming) and *scenario* (autonomous driving, road safety, traffic management, infotainment). As shown in Figure 2, the mean values of the four measures vary across the conditions or scenarios.

To quantify the effect, we first construct a Cumulative Link Mixed-effects Model (CLMM) for each measure with "clmm" function from the "ordinal" package [31]. We chose CLMM because of the ordinal nature of the scale ratings for each measure and its modeling of random effects. We model each measure as the dependent variable and took the two main effects and their two-way interaction as the fixed effect. To account for the within-subject design and the scenario randomly selected for each category, we also took the participant ID and scenario ID as the random effect. We report χ^2 values and corresponding p values for each model. To further quantify the effect's direction and magnitude, we report estimated coefficients (β) and corresponding p values of significant terms. Complete regression results are shown in Table 3. We conducted null-hypothesis testing ($\alpha = 0.05$) for those measures. The null hypothesis was rejected when the obtained results among the conditions were significantly different from each other. Parametric tests such as ANOVA are robust to yield the right answer even when distributional assumptions are violated [18, 80]. We also constructed a linear mixed-effects regression (or LMER) for each model and obtained results consistent with CLMMs (see Appendix A.2).

At Phase 3, we measured participants' experience in using connectivity and driving assistance functions. Based on the their responses, we categorized their experience into three levels: *little* (151 "never" or "rarely" used either function), *some* (240 "sometimes" or "often" use at least one of the functions), *much* (204 "sometimes" or "often" use both functions). We conducted the CLMMs same as Phase 2 but added *experience* (little, some, much) as another factor for each measure.

[1]We ran a pilot survey on MTurk with 20 participants to decide the expected time. Our payment was based on federal minimal wage $7.25.

[2]The final participant number was slightly smaller than 606 (the suggested participant number through power analysis), the power we achieved was .793.



(a) Perceived Benefits of Data Sharing

(b) Perceived Risks of Data Sharing

(c) Willingness to Share

(d) Confidence of Sharing Decision

Figure 2: Results of four measures at Phase 2 as a function of **Scenario** (infotainment, traffic management, road safety and autonomous driving) and **Condition** (control, privacy priming, privacy&security priming). Numbers in the parentheses indicate the number of participants in each condition. The error bars represent 2 standard errors.

4.1 Perceived Benefits and Risks

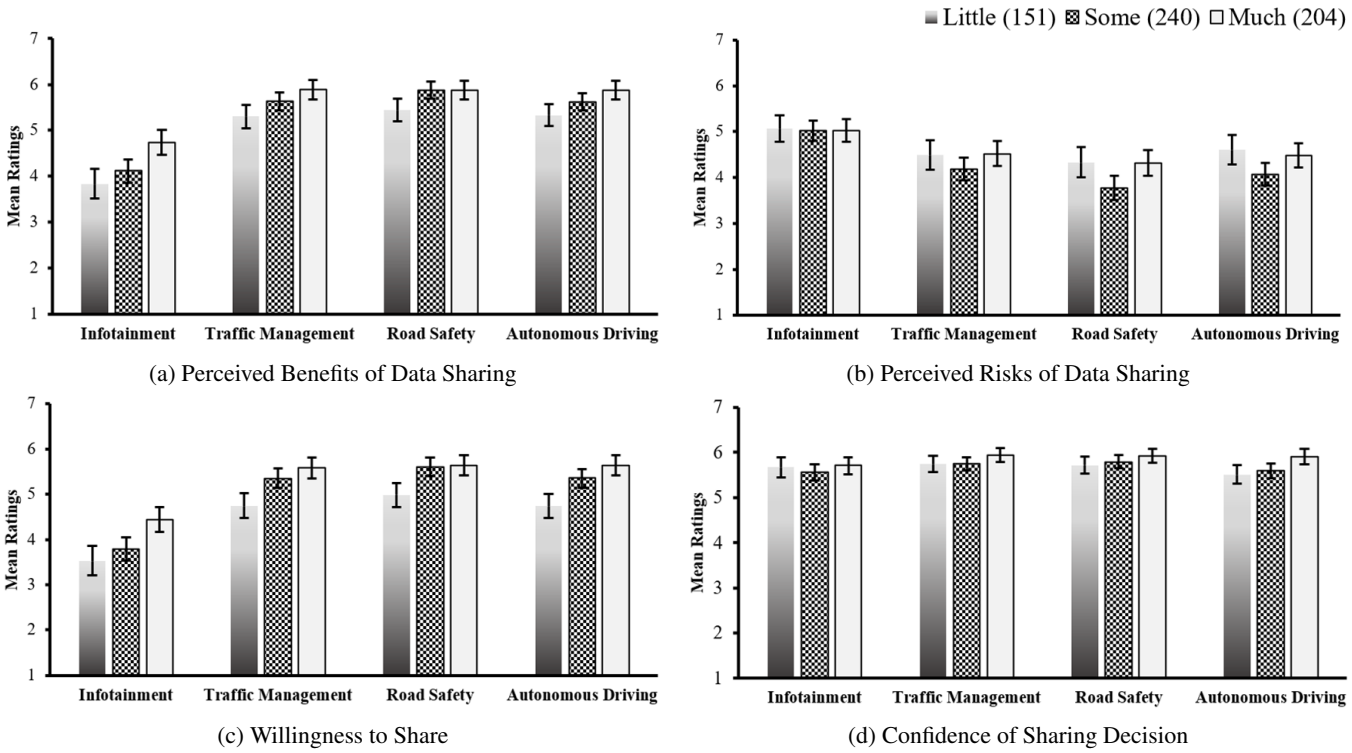
Sharing Data. The CLMM results confirmed that both *scenario*, $\chi^2(3) = 50.14$, $p < .001$, and *condition*, $\chi^2(2) = 7.84$, $p = .020$, had an significant effect on the perceived benefits (see Figure 2a). In the CLMMs, the control condition and the infotainment scenario are the baseline condition and scenario, respectively. Generally, participants perceived more benefits for sharing data in the driving-related scenarios (i.e., traffic management, road safety, autonomous driving) than in the infotainment scenarios ($\beta_s > 1.708, p_s < .001$), consistent with previous findings (e.g., [20, 53]). Compared to the control condition, only participants in the privacy-priming condition perceiving fewer benefits ($\beta = -0.736, p < .01$). The two-way interaction of scenario $\times$ condition was also significant, $\chi^2(6) = 15.62$, $p = .016$, mainly because participants in the privacy&security-priming condition perceived more benefits for the traffic management scenario than those in the control condition for the infotainment scenario ($\beta = 0.580, p < .05$).

For the perceived risks, participants gave an average rating larger than 4 (see Figure 2b), indicating that they were aware of privacy risks in each scenario. The main effect of scenario was significant, $\chi^2(3) = 33.17$, $p < .001$. In agreement with the results of perceived benefits, the participants perceived fewer risks in the driving-related scenarios than in the infotainment scenarios ($\beta_s < -0.697, p_s < .01$). Nevertheless, the main effect of condition and its interaction with scenario were not significant, $\chi^2_s < 4.22, p_s > .176$, revealing limited impacts of the priming effect on risk perception.

Finding 1: *While users perceived more benefits but fewer risks in the driving-related scenarios, they perceived more risks but fewer benefits in the infotainment scenarios. Such opposite patterns reveal the relatively heavier weighting of driving-relevant information than otherwise, implying a privacy-safety tradeoff in the CAV context (**RQ1**).*

Receiving Data. The main effect of scenario was significant for the perceived benefits, $\chi^2(3) = 47.50$, $p < .001$ and risks, $\chi^2(3) = 40.71$, $p < .001$, of receiving data in the privacy&security-priming condition. Consistent with the sharing-data results, participants perceived more benefits ($\beta_s > 2.034, p_s < .001$) but fewer risks ($\beta_s < -0.989, p_s < .001$) in the other three scenarios than in the infotainment scenario. We also did an exploratory analysis to understand possible differences between sharing and receiving data . The participants perceived more benefits, $\chi^2(1) = 6.36$, $p = .012$, but fewer risks, $\chi^2(1) = 18.91$, $p < .001$, in receiving data than sharing data. Such pattern was consistent across the four scenarios, $\chi^2_s(3) < 1.51, p_s > .680$, indicating that participants might have focused on the benefits but underestimated the risks associated with receiving data.

Finding 2: *Only the privacy priming was effective in reduc-*



(a) Perceived Benefits of Data Sharing

(b) Perceived Risks of Data Sharing

(c) Willingness to Share

(d) Confidence of Sharing Decision

Figure 3: Results of four measures at Phase 2 as a function of **Scenario** (infotainment, traffic management, road safety and autonomous driving) and **Experience** (little, some, much). Numbers in the parentheses indicate the number of participants at each experience level. The error bars represent 2 standard errors.

*ing CAV users' perceived benefits than those in the control. Instead of augmenting CAV users' privacy concerns, the privacy&security priming condition showed similar results as those in the control, probably due to more benefits and fewer risks perceived in receiving data than sharing data (**RQ2**).*

4.2 Willingness to Share and Confidence

Participants' willingness to share data varied across scenarios, $\chi^2(3) = 52.43$, $p < .001$, and conditions, $\chi^2(2) = 7.49$, $p = .024$ (see Figure 2c). They showed more data-sharing willingness for the driving-related scenarios than for the infotainment scenarios ($\beta_s > 1.806, p_s < .001$). In addition, participants in the control condition were more willing to share data than those in the two priming conditions ($\beta_s < -0.660, p_s < .05$). Thus, compared to the perceived benefits or risks, the priming effect was more obvious in the data-sharing decisions. No interaction effect was observed, $\chi^2(6) = 9.21$, $p = .162$, indicating the priming effect is not scenario-dependent.

Participants were confident about their data-sharing decisions in general (see Figure 2d). The main effect of scenario was significant, $\chi^2(3) = 8.39$, $p = .039$. Yet, relative to the infotainment scenario (baseline), no significant differences were obtained ($\beta_s < 0.378, p_s > .05$). Neither the main effect of condition, $\chi^2(2) = 4.73, p = .094$, nor its interaction with scenario, $\chi^2(6) = 11.65, p = .070$, were significant, suggesting limited influence of priming for their decision confidence.

Finding 3: *CAV users made more liberal privacy decisions in the driving-related scenarios, which could have been caused by perceiving both more benefits and fewer risks (**RQ1**). Moreover, they made more conservative privacy decisions as long as they were primed (**RQ2**).*

4.3 Effect of Prior Experience

Figure 3 shows a trend that users with *much* experience in driving assistance and connectivity functions perceived more benefits and risks, and showed more willingness to share data. We explore the effect of their prior experience by adding it as another factor in the CLMMs. We set the *little* experience as the baseline and report significant terms involving experience.

The main effect of prior experience was significant in participants' perceived benefits, $\chi^2(2) = 17.57$, $p < .001$, perceived risks, $\chi^2(2) = 8.21$, $p = .017$, and their willingness to share data, $\chi^2(2) = 28.87$, $p < .001$. Yet, neither *some* nor *much* experience levels showed any significant differences compared to the baseline for each measure (benefits: $\beta_s < 0.320$, $p_s > .05$; risks: $\beta_s < 0.377$, $p_s > .05$; willingness: $\beta_s < 0.868, p_s > .05$). There was an interaction effect of scenario $\times$ experience, $\chi^2(6) = 13.48$, $p = .036$, but no significant differences were obtained relative to the baseline.

Table 3: **Effects of Condition and Scenario on Four Measures.** We build each CLMM by considering the two main effects and their interaction. Significance is denoted by *** ($p < 0.001$), ** ($p < 0.01$), and * ($p < 0.05$).

	Perceived Benefits			Perceived Risks			Willingness to Share			Confidence of Sharing Decision		
Random Effect	**Variance**	**Std. Dev.**		**Variance**	**Std. Dev.**		**Variance**	**Std. Dev.**		**Variance**	**Std. Dev.**	
Participant ID	3.164	1.779		3.968	1.992		4.737	2.176		2.689	1.640	
Scenario ID	0.237	0.486		0.082	0.287		0.245	0.495		0.008	0.091	
Variable	**Estimate (β)**	**Std. Err.**	***p***	**Estimate (β)**	**Std. Err.**	***p***	**Estimate (β)**	**Std. Err.**	***p***	**Estimate (β)**	**Std. Err.**	***p***
Condition (Reference = Control)												
Privacy Priming	-0.736	0.257	.004**	0.656	0.272	.016*	-0.683	0.287	.017*	0.130	0.254	.608
Privacy&Security Priming	-0.453	0.267	.090	0.466	0.282	.098	-0.660	0.297	.026*	0.014	0.263	.957
Scenario (Reference = Infotainment)												
Traffic Management	1.708	0.392	<.001***	-0.697	0.270	.010**	1.806	0.398	<.001***	0.336	0.198	.089
Road Safety	2.177	0.394	<.001***	-1.053	0.271	<.001***	2.316	0.400	<.001***	0.378	0.196	.054
Autonomous Driving	2.078	0.393	<.001***	-0.778	0.270	.004**	2.079	0.398	<.001***	0.228	0.196	.244
Condition : Scenario (Reference = Control : Infotainment)												
Privacy : Traffic Management	0.433	0.268	.106	-0.311	0.260	.233	0.315	0.270	.243	0.012	0.274	.966
Privacy&Security : Traffic Management	0.580	0.278	.037*	-0.356	0.268	.184	0.415	0.278	.135	-0.269	0.281	.337
Privacy : Road Safety	0.451	0.273	.099	-0.436	0.264	.098	0.395	0.275	.152	0.351	0.275	.203
Privacy&Security : Road Safety	-0.107	0.279	.702	-0.198	0.270	.463	-0.114	0.278	.683	-0.510	0.280	.069
Privacy : Autonomous Driving	-0.086	0.267	.747	-0.295	0.260	.257	0.166	0.269	.537	-0.205	0.272	.452
Privacy&Security : Autonomous Driving	-0.270	0.277	.329	-0.293	0.268	.274	-0.175	0.277	.527	-0.324	0.279	.246
Threshold Coefficient	**Estimate**	**Std. Err.**		**Estimate**	**Std. Err.**		**Estimate**	**Std. Err.**		**Estimate**	**Std. Err.**	
1|2	-3.369	0.322		-4.395	0.264		-3.337	0.332		-6.389	0.360	
2|3	-2.104	0.309		-2.338	0.244		-1.843	0.320		-4.805	0.243	
3|4	-1.372	0.305		-1.415	0.239		-1.089	0.318		-3.531	0.206	
4|5	-0.694	0.304		-0.734	0.238		-0.246	0.317		-2.397	0.191	
5|6	0.500	0.304		0.469	0.238		1.043	0.318		-0.978	0.184	
6|7	2.654	0.309		2.092	0.243		3.464	0.327		1.514	0.185	

Finding 4: *We observed a non-significant trend that users with much experience in driving assistance and connectivity functions perceived more benefits and more risks of data sharing, suggesting that they might have a better understanding of the pros and cons of the described V2X functions. Still there was a non-significant trend that they showed higher willingness in sharing the data, implying that their data-sharing decisions were more aligned with perceived benefits (**RQ3**).*

4.4 Privacy Attitudes and Trust

In the post-session questionnaire, we examined participants' privacy attitude with a subset of IUIPC (11 questions), which is typically used to understand people's general privacy attitude toward online information [74]. We averaged participant's ratings of the 11 questions to get a score for their privacy attitude. The participants had strong concerns about their own privacy regardless of the conditions[3] (control: 6.1; privacy priming: 6.1; privacy&security priming: 6.1; $F < 1.0$). Since the IUIPC questions were asked at the end of the survey, the non-significant differences across conditions could indicate that participants might have raised similar privacy concerns after answering questions at Phase 2. Participants' trust in the V2X communication was also similar across conditions[4] (control: 3.58; privacy priming: 3.41; privacy&security priming: 3.40; $\chi^2(2) = 5.63$, $p = .060$).

4.5 Response to Open-ended Questions

After participants indicated their willingness and confidence to share the data in each scenario, we asked them to describe factors that they considered when making the decisions. We did a thematic analysis [15] for the 2293 meaningful answers. Two coders analyzed half of the data independently at first and then developed a code book through iterative discussions. Then they revised their codes and coded the other half data independently. Therefore, every answer was coded by both coders. The inter-coder agreement via Cohen's Kappa was 0.93, indicating a high agreement [64]. The two coders resolved the discrepancies between them by revisiting the criteria over multiple discussions. Then they discussed the results and finalized the thematic analysis together. Note that a single response may have multiple themes. We identified **five major themes** and described the numerical difference across scenarios:

Benefits, especially safety, come prior to privacy (55.0%). Such a top theme showed that when participants made data-sharing decisions, the majority of them considered the benefits (convenience and safety). For example, **P10** answered, "*I think the benefits [of trip planning] outweigh any concerns I'd have [for] sharing this data.*" We examined the theme across the four scenarios. Consistent with the quantitative results reported earlier, the difference across scenarios were mainly revealed by more emphasizes on the benefits in the three driving-related scenarios (59.7%, 66.1%, 61.7%) than in the infotainment scenarios (31.8%). Moreover, about 14.3% of the participants mentioned *safety* in their responses specifically. For instance, **P343** described "*Safety comes prior to concerns for privacy [concerns]. If it will help me with my safety and health, I don't mind sharing my private information.*" Such pattern was more evident in the three driving-related scenarios (9.9%, 20.2%, 21.6%) than the infotainment scenarios (5.2%).

Privacy concerns (29.8%). Participants had privacy con-

[3] Participants' privacy attitude was analyzed with one-way ANOVA.
[4] Trust was analyzed with Kruskal–Wallis one-way analysis of variance.

cerns when making the data-sharing decision. For example, **P218** answered that "*I don't know enough yet to commit. But, it sounds really promising, I just have concerns about the seemingly complete knowledge of every move I make, who else has access, how long it is stored, and if it can be accessed without my permission or knowledge by any person or any agency.*" Those privacy concerns varied across scenarios, showing more concerns in the infotainment scenarios (37.7%) than in the other scenarios (27.2%, 23.1%, 31.3%).

Common good (13.4%). Some participants were willing to share the data because it could be beneficial to others, especially for the three driving-related scenarios (18.7%, 16.4%, 15.5%) than for the remaining one (2.9%). For instance, **P1** replied: "*Sharing this data will make the roads safer for everyone so I feel a responsibility to do so.*" Notice that some participants might have implicitly indicated this theme by describing the application as "beneficial." Thus, the number reported here might be underestimated. We did not double count responses mentioning "common good" into "Benefits come prior to privacy" theme either.

Insensitive data or expectation of protected data sharing (13.3%). Some participants revealed wrong perception about data sharing in the CAV context (e.g., "*This is pretty standard data that doesn't feel intrusive to ME at all. It seems to be a lot of data just about my vehicle, which isn't a big deal to me. And then in terms of "other" data like my vehicle location, that doesn't seem that much different than when I'm using my GPS or anything like that, so I don't necessarily have a problem with it*"(**P71**)). Some participants explicitly expected data in the CAV setting to be temporary (e.g., "*I understand collecting this short-term data for road safety and it makes sense to me as it could greatly reduce accidents. Also, I would not think these data would need to be kept for the long-term*"(**P530**)) and processed with sufficient protection measures (e.g., "*I would trust that security software will be developed to allow this service to be safe and not allow others to get sensitive information*"(**P106**)). Unsurprisingly, those trends were more evident in the three driving-related scenarios (14.0%, 15.5%, 13.9%) than the infotainment scenario (9.8%).

Not beneficial or unnecessary (11.8%). Compared to the driving-related scenarios (5.6%, 7.3%, 4.1%), about 30.8% of responses in the infotainment scenarios indicated that participants did not share the data because they perceived limited benefits (e.g., "*The service offered is a waste of my time, money, and energy. When I am driving I enjoy the scenery, the experience, and if traveling with others I am enjoying their company. Fiddling with gadgets is avoiding the joy of driving and travel*"(**P501**)). Some participants declined to use functions already implemented in other devices (e.g., "*I don't see a benefit in such service [find facilities nearby and receiving information of services and prices] since my cell phone provides me exactly with the same information whenever I need it*"(**P257**)).

The other themes we identified in the coding process are *security concern* (4.1%), *government's / companies' abuse of data* (3.8%), and *public information* (3.1%). Data abuse and security risks can be considered as specific examples and consequences of privacy breach. Related to the theme of "insensitive data," participants indicated that the required data were already public, which may have contributed to their belief of data being insensitive.

We also observed two extra themes in small percentage (about 1-2% on average) but somewhat *unique* to the CAV context. First, several participants were unsure about their intention and indicated they need to know more about the technology, data type and safety measure, suggesting an unfamiliarity of CAV data sharing (e.g., "*I think this technology is very new to me, I need to get to know it better and find out about my data and my privacy*"(**P203**)). Second, participants mentioned that data sharing (e.g., destination and location) can be more risky if they were carrying other passengers in the vehicle, suggesting their final decision may vary (e.g., "*Sharing destinations with other individuals or entities can be a safety risk, especially if I am carrying other passengers in the vehicle. It is not worth the tradeoff to me*"(**P248**)).

Finding 5: *Our thematic analysis verified the privacy-safety tradeoff. The analysis revealed not only common factors similar to other settings, but also some unique factors for the CAV context (**RQ1**).*

5 General Discussion

We conducted an online vignette study with 16 V2X communication scenarios to examine participants' perceived benefits and risks of various data exchanges in the CAV context. We also measured the participants' data-sharing decisions and their decision confidence. Compared to the infotainment scenarios, our results showed that the participants perceived more benefits but fewer risks in the driving-related scenarios (i.e., traffic management, road safety, and autonomous driving), and consequently were more willing to share their data. Moreover, participants' data-sharing decisions were subject to change due to other factors such as privacy priming or their prior experience in driving assistance and connectivity functions.

Next, we discuss possible explanations of the obtained results and interventions to facilitate privacy behavior in the CAV context. We then discuss recommendations for practitioners, the limitations of our study and future research directions.

5.1 Privacy Behavior in the CAV Context

A take-home message of our study is that *benefits* plays a critical role in users' CAV privacy decision-making. Besides privacy-utility tradeoff (e.g., parking convenience), we obtained privacy-safety tradeoff across different driving-related

scenarios (Finding 1). Responses to the open-ended questions also verified the critical role of *safety* in their decision-making.

Tradeoffs of Privacy-Utility and Privacy-Safety. The notion of privacy calculus indicates that when asked to provide personal information to service providers or companies, users perform a cost-benefit analysis [34]. In our experiment, perceived risks of data sharing were negatively correlated with perceived benefits. The participants were more likely to share the data (i.e., accept the potential risks that accompany the disclosure of personal information) as long as they perceived that benefits exceeded the costs of disclosure [33] (e.g., safety outweighs privacy in driving-related scenarios).

Beyond safety concerns about themselves, the participants also indicated that they made the sharing decision due to the safety concerns about others on the road (Finding 5). Such results are consistent with previous findings in manual driving context, indicating the *altruistic* aspect of driving [77]. Some of the participants also considered the privacy of passengers inside the vehicles, indicating the role of *social* aspect in the CAV privacy decision-making.

Effects of Prior Experience. We found the main effect of participants' prior experience of driving assistance and connectivity functions in their perception of benefits and risks, as well as their data-sharing willingness. Such results were consistent with Brell et al. [17], which found that participants' prior experience with driving assistance systems (e.g., automatic parking and cruise control) had a significant influence on the perceived benefits of using CAVs and risks concerning data collection and use. Relative to the participants with *little* experience (baseline), those with more experience (*some* and *much*) only revealed nonsignificant increasing trends. Moreover, the more willingness to share data even when perceiving more risks suggests that CAV users with more relevant experience are likely to be attracted by the utility but neglect the potential privacy risks of sharing data. Thus, besides learning from *experience*, it is critical to equip users with the correct *knowledge* of CAV data collection and use. In addition, the nonsignificant differences relative to baseline could be caused by various factors. For example, the number of participants was probably not large enough to detect the statistically significant differences among varied experience levels.

5.2 Privacy Risk Communication of V2X

Our study results (Findings 2-4) provide insights into how to use priming to remind users about privacy risks in the CAV context. Presenting users with privacy risks *prior to* the data-sharing decision is effective in increasing conservative privacy decision-making. Such results are consistent with the literature on the app selection [29, 84] and the IoT setting [67]. Different from the mobile setting [29], the individual differences among participants with relevant CAV experiences indicate that interventions in the CAV context might need to be customized to lead them to think about their privacy differently. For example, concrete priming items in each scenario or personal- or self-relevant information [84] could be considered to promote safer data-sharing decisions for users with much relevant experience.

Ineffectiveness of Security Priming. Out of our expectations, instead of reducing perceived benefits and increasing perceived risks, additional security priming somehow resulted in ratings between the control and the privacy-priming conditions. Thus, the presentation of *receiving data* in the security priming might have mainly increased participants' perceived benefits. Although we highlighted possible security risks when receiving information, participants might have thought of them separately from the privacy risks of *sharing data*. Considering the *cooperation* aspect in driving, such results raise *novel* challenges of usable privacy in the CAV context. Alternatively, such results might indicate that participants were less aware of security risks than privacy risks throughout the data exchange. As noted by participants' answers to the open-ended questions, effective training that helps CAV users understand the technology and the implications to data privacy and security seems to be essential.

Transparent Privacy-enhancing Technology of CAVs. Several participants revealed expectations of strong privacy protections in the CAV context, suggesting the importance of communicating privacy-enhancing technology of CAVs to encourage safer data sharing. Such results were consistent with demand of preventative measures to prevent security breaches in autonomous driving [45]. Salazer et al. [86] recently proposed V2X Core Anomaly Dectection System (VCADS) to validate the V2X messages beyond authentication. The authors performed evaluations on V2X field-testing datasets and attack simulations, and found that VCADS were able to detect more than 85% of attacks. Nevertheless, it is unclear 1) whether the proposed protection meets users' *expectations*, and 2) whether users could *understand* and *trust* the proposed system. To ensure the usability of such state-of-the-art privacy technology, future work could consider a evaluation including CAV users throughout the design and development processes.

5.3 Recommendations for Practitioners

We believe that automobile OEMs and policymakers can significantly contribute to the human aspects of privacy of V2X communication for CAVs by considering the following facets.

Privacy Risk Communication, Policies, and Regulations. Drivers were concerned about sharing data in V2X communication for CAVs; yet, they placed benefits, especially safety, prior to privacy. Thus, automobile companies should develop privacy policies in terms of effectively communicating privacy risks of V2X communication. For example, we recommend communicating both general privacy risks and specific privacy implications [68] of V2X communication, such that they become more visible and accessible for users. Also, policies and regulations at other levels (e.g., government) should focus

on the tradeoff between safety and privacy of data sharing for V2X communication. Specifically, the data collection and corresponding privacy risks should be explicit to the public.

Privacy-enhancing Technology. Users revealed expectations about protected data sharing. A significant body of work has been conducted to ensure privacy for vehicular communication systems [72], focusing on identity privacy and location privacy. Yet, anonymity is not sufficient since location data are highly correlated and driving locations based on traffic rules are very predictable [4]. For example, the effectiveness of anonymous authentication has been questioned by successful tracking attacks in the simulator based on beacon messages [103]. Thus, more advanced technologies, such as differential privacy (DP [35]) could be considered to maintain the trajectory privacy and utility simultaneously [14, 26, 41, 50].

V2X and CAV Training. Incorrect perception of data sharing in CAVs highlights that consumer education and training should be considered and provided by automobile companies and government agencies. We recommend approaches such as driving simulator training [58] to facilitate understanding of both *what* and *how* aspects of V2X communication in CAVs.

5.4 Limitations

There are a few limitations in our study method. *First*, we recruited MTurk workers who tend to be young, more educated, and more aware of privacy issues [57]. Our participants were diverse in demographics but they may not represent the U.S. population. Our study was conducted in the U.S., thus the obtained results may not necessarily represent privacy perception and decision of CAVs in other regions (e.g., EU or East Asia). *Second*, we introduced CAVs and V2X at the beginning of our survey, but it was still possible that those concepts were obscure to the participants. The functions described are far from real applications, which could have led to difficulties for the participants to precisely evaluate and compare the benefits and risks. *Third*, our result may be limited to attentive users or those with higher reading comprehension since they are more likely to pass the comprehension test.

Fourth, we did not include filler to make the text length equivalent between the two priming manipulations. Despite more information in the privacy&security priming condition, participants spent similar time completing the survey (Control: 947 s; Privacy: 890 s; Privacy&Security: 950 s, $p = .170$). Moreover, we focused on the impact of the text descriptions on the following privacy perceptions and decisions. The results were similar to those of the privacy priming condition, suggesting limited impacts of the text length. *Fifth*, we only randomly sampled one scenario for each V2X application. Future work could consider increasing the sample size in each to increase the internal validity. *Lastly*, we presented the priming manipulations in two of three conditions initially, but the following V2X communication scenarios were service-oriented. Thus, participants might have focused on benefits rather than risks when making the judgments and the decisions.

5.5 Future Research Directions

Our study findings can only serve as the basis for more systematic studies regarding human aspects of privacy of V2X communication for CAVs. *First*, we suggest users' privacy perception and decision should be investigated in a setting with higher ecological validity. For example, future work could consider using video [45], a driving simulator, or AR/VR to give users the *experience* of V2X communication for CAVs. Such studies could leverage the scenarios that we constructed to create appropriate driving contexts to explore the differences among scenarios. *Second*, individuals' stated disclosure intentions could vary from their actual data-sharing behaviors [10, 40]. We argue that such privacy paradox [79]) should be investigated to obtain a more comprehensive understanding of privacy behavior in CAVs. *Third*, our study mainly focuses on data exchanges with other vehicles (V2V) or the transport infrastructure (V2I) [63]. Future studies could consider other service purposes or data collection and use (e.g., V2P). Data exchanges in V2X communication have extra unique challenges for usable privacy. For instance, CAVs normally drive at high speed. Any decision regarding V2X communication will be *time*- and *response*-critical [59]. Also, the sheer number of possible encountered vehicles and entities could create issues such as choice *overload* for privacy control, making it hard to track the information flow in *real time*. We recommend further research to explore those novel problem spaces.

6 Conclusion

The rapid development of CAVs will make them available to most users in the near future [69]. Our results reveal that users have privacy concerns about V2X communication in the CAV context but they are more likely to be attracted by the explicit benefits and safety considerations. We suggest service providers should inform users of the privacy risks and implications of the collected data such that the users can reach a comprehensive decision about using a service. We also found that users' prior experience on driving assistance and connectivity functions could lead to varied privacy perceptions and decisions, suggesting that individually tailored privacy design may need to be considered for CAVs. Our thematic analysis results also offer insights to policy makers for effectively communicating privacy of V2X communication.

Acknowledgments

This work was funded in part by a seed grant from Penn State's Center for Security Research and Education (CSRE) and NSF award #1931441. We also thank Ziyan An and Jie Zhu for their help in survey design and thematic analysis.

References

[1] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. Privacy and human behavior in the age of information. *Science*, 347(6221):509–514, 2015.

[2] Alessandro Acquisti and Jens Grossklags. Privacy and rationality in individual decision making. *IEEE Security & Privacy*, 3(1):26–33, 2005.

[3] Claudio Agostino Ardagna, Marco Cremonini, Ernesto Damiani, S De Capitani di Vimercati, and Pierangela Samarati. Location privacy protection through obfuscation-based techniques. In *IFIP Annual Conference on Data and Applications Security and Privacy*, pages 47–60. Springer, 2007.

[4] Philip Asuquo, Haitham Cruickshank, Jeremy Morley, Chibueze P Anyigor Ogah, Ao Lei, Waleed Hathal, Shihan Bao, and Zhili Sun. Security and privacy in location-based services for vehicular and mobile communications: an overview, challenges, and countermeasures. *IEEE Internet of Things Journal*, 5(6):4778–4802, 2018.

[5] Ugur I Atmaca, Carsten Maple, and Mehrdad Dianati. Emerging privacy challenges and approaches in cav systems. In *Living in the Internet of Things (IoT 2019)*, pages 1–9. IET, 2019.

[6] Maria Azees, Pandi Vijayakumar, and Lazarus Jegatha Deboarh. Eaap: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems*, 18(9):2467–2476, 2017.

[7] Claudine Badue, Rânik Guidolini, Raphael Vivacqua Carneiro, Pedro Azevedo, Vinicius B Cardoso, Avelino Forechi, Luan Jesus, Rodrigo Berriel, Thiago M Paixao, Filipe Mutz, et al. Self-driving cars: A survey. *Expert Systems with Applications*, 165:113816, 2021.

[8] Rebecca Balebako, Pedro G Leon, Hazim Almuhimedi, Patrick Gage Kelley, Jonathan Mugan, Alessandro Acquisti, Lorrie Cranor, and Norman Sadeh-Koniecpol. Nudging users towards privacy on mobile devices. In *Proceedings of CHI-PINC*. Carnegie Mellon University, 2011.

[9] Walter Balzano and Fabio Vitale. Dig-park: A smart parking availability searching method using v2v/v2i and dgp-class problem. *2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, pages 698–703, 2017.

[10] Susanne Barth and Menno DT De Jong. The privacy paradox–investigating discrepancies between expressed privacy concerns and actual online behavior–a systematic literature review. *Telematics and Informatics*, 34(7):1038–1058, 2017.

[11] Douglas Bates, Martin Maechler, Ben Bolker, Steven Walker, Rune Haubo Bojesen Christensen, Henrik Singmann, Bin Dai, Fabian Scheipl, and Gabor Grothendieck. Package 'lme4'. *Linear mixed-effects models using S4 classes. R package version*, 1(6), 2011.

[12] Cara Bloom, Joshua Tan, Javed Ramjohn, and Lujo Bauer. Self-driving cars and data collection: Privacy perceptions of networked autonomous vehicles. In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*, pages 357–375, 2017.

[13] Toby Bolsen, James N Druckman, and Fay Lomax Cook. The influence of partisan motivated reasoning on public opinion. *Political Behavior*, 36(2):235–262, 2014.

[14] Luca Bonomi and Li Xiong. A two-phase algorithm for mining sequential patterns with differential privacy. In *Proceedings of the 22nd ACM international conference on Information & Knowledge Management*, pages 269–278, 2013.

[15] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2):77–101, 2006.

[16] Teresa Brell, Hannah Biermann, Ralf Philipsen, and Martina Ziefle. Conditional privacy: Users' perception of data privacy in autonomous driving. In *VEHITS*, pages 352–359, 2019.

[17] Teresa Brell, Ralf Philipsen, and Martina Ziefle. scary! risk perceptions in autonomous driving: The influence of experience on perceived benefits and barriers. *Risk Analysis*, 39(2):342–357, 2019.

[18] Aenne A Brielmann, Angelica Nuzzo, and Denis G Pelli. Beauty, the feeling. *Acta Psychologica*, 219:103365, 2021.

[19] Holger Caesar, Varun Bankiti, Alex H. Lang, Sourabh Vora, Venice Erin Liong, Qiang Xu, Anush Krishnan, Yu Pan, Giancarlo Baldan, and Oscar Beijbom. nuscenes: A multimodal dataset for autonomous driving, 2020.

[20] Zekun Cai and Aiping Xiong. Effects of knowledge and experience on privacy decision-making in connected autonomous vehicle scenarios. In *Proceedings of the Workshop on Usable Security (USEC'22)*, pages 1–18, 2022.

[21] Zekun Cai and Aiping Xiong. Supplementary materials. https://github.com/MandiaCai/V2X-Survey, 2022.

[22] Erin Carbone and George Loewenstein. Dying to divulge: The determinants of, and relationship between, desired and actual disclosure. *Desired and Actual Disclosure (May 28, 2020)*, 2020.

[23] Daphne Chang, Erin L Krupka, Eytan Adar, and Alessandro Acquisti. Engineering information disclosure: Norm shaping designs. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 587–597, 2016.

[24] J Chang, G Hatcher, D Hicks, J Schneeberger, B Staples, S Sundarajan, M Vasudevan, P Wang, K Wunderlich, et al. Estimated benefits of connected vehicle applications: dynamic mobility applications, aeris, v2i safety, and road weather management applications. Technical report, United States. Department of Transportation. Intelligent Transportation Systems Joint Program Office, 2015.

[25] Jing Chen, Christopher S Gates, Ninghui Li, and Robert W. Proctor. Influence of risk/safety information framing on android app-installation decisions. *Journal of Cognitive Engineering and Decision Making*, 9(2):149–168, 2015.

[26] Rui Chen, Benjamin CM Fung, Bipin C Desai, and Nériah M Sossou. Differentially private transit data publication: a case study on the montreal transportation system. In *Proceedings of the 18th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pages 213–221, 2012.

[27] Shanzhi Chen, Jinling Hu, Yan Shi, Ying Peng, Jiayi Fang, Rui Zhao, and Li Zhao. Vehicle-to-everything (V2X) services supported by LTE-based systems and 5G. *IEEE Communications Standards Magazine*, 1(2):70–76, 2017.

[28] Eun Kyoung Choe, Jaeyeon Jung, Bongshin Lee, and Kristie Fisher. Nudging people away from privacy-invasive mobile apps through visual framing. In *IFIP Conference on Human-Computer Interaction*, pages 74–91. Springer, 2013.

[29] Isis Chong, Huangyi Ge, Ninghui Li, and Robert W. Proctor. Influence of privacy priming and security framing on mobile app selection. *Computers & Security*, 78:143–154, 2018.

[30] Abdullahi Chowdhury, Gour Karmakar, Joarder Kamruzzaman, Alireza Jolfaei, and Rajkumar Das. Attacks on self-driving cars and their countermeasures: A survey. *IEEE Access*, 8:207308–207342, 2020.

[31] Rune Haubo B Christensen. A tutorial on fitting cumulative link mixed models with clmm2 from the ordinal package. *Tutorial for the R Package ordinal https://cran. r-project. org/web/packages/ordinal/Accessed*, 1, 2019.

[32] European Commission. Connected and automated mobility. https://digital-strategy.ec.europa.eu/en/policies/connected-and-automated-mobility, 2020.

[33] Mary J Culnan and Robert J Bies. Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues*, 59(2):323–342, 2003.

[34] Tamara Dinev and Paul Hart. An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1):61–80, 2006.

[35] Cynthia Dwork. Differential privacy. In *ICALP*, pages 1–12, 2006.

[36] Pardis Emami-Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. Privacy expectations and preferences in an iot world. In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*, pages 399–412, 2017.

[37] Franz Faul, Edgar Erdfelder, Albert-Georg Lang, and Axel Buchner. G* power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior Research Methods*, 39(2):175–191, 2007.

[38] Janet Finch. The vignette technique in survey research. *Sociology*, 21(1):105–114, 1987.

[39] Andreas Geiger, Philip Lenz, and Raquel Urtasun. Are we ready for autonomous driving? the kitti vision benchmark suite. In *2012 IEEE Conference on Computer Vision and Pattern Recognition*, pages 3354–3361, 2012.

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

[41] Soheila Ghane, Lars Kulik, and Kotagiri Ramamohanarao. Tgm: A generative mechanism for publishing trajectories with differential privacy. *IEEE Internet of Things Journal*, 7(4):2611–2621, 2019.

[42] Amrita Ghosal and Mauro Conti. Security issues and challenges in v2x: A survey. *Computer Networks*, 169:107093, 2020.

[43] Robert L Goldstone, Joshua R de Leeuw, and David H Landy. Fitting perception in and to cognition. *Cognition*, 135:24–29, 2015.

[44] Leo A Goodman. Snowball sampling. *The Annals of Mathematical Statistics*, pages 148–170, 1961.

[45] Lea Theresa Gröber, Matthias Fassl, Abhilash Gupta, and Katharina Krombholz. Investigating car drivers' information demand after safety and security critical incidents. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–17, 2021.

[46] Chunshi Guo, Chouki Sentouh, Jean-Christophe Popieul, Jean-Baptiste Haué, Sabine Langlois, Jean-Jacques Loeillet, Boussaad Soualmi, and Thomas Nguyen That. Cooperation between driver and automated driving system: Implementation and evaluation. *Transportation Research Part F: Traffic Psychology and Behaviour*, 61:314–325, 2019.

[47] Jens Hainmueller, Dominik Hangartner, and Giuseppe Pietrantuono. Naturalization fosters the long-term political integration of immigrants. *Proceedings of the National Academy of Sciences*, 112(41):12651–12656, 2015.

[48] Il-Horn Hann, Kai-Lung Hui, Sang-Yong Tom Lee, and Ivan PL Png. Overcoming online information privacy concerns: An information-processing theory approach. *Journal of Management Information Systems*, 24(2):13–42, 2007.

[49] Marian Harbach, Markus Hettig, Susanne Weber, and Matthew Smith. Using personal examples to improve risk communication for security & privacy decisions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2647–2656, 2014.

[50] Xi He, Graham Cormode, Ashwin Machanavajjhala, Cecilia M Procopiuc, and Divesh Srivastava. Dpt: differentially private trajectory synthesis using hierarchical reference systems. *Proceedings of the VLDB Endowment*, 8(11):1154–1165, 2015.

[51] Mathias Heesen, Martin Baumann, Johann Kelsch, Daniel Nause, and Max Friedrich. Investigation of cooperative driving behaviour during lane change in a multi-driver simulation environment. In *Human Factors and Ergonomics Society (HFES) Europe Chapter Conference Touluse*, pages 305–318, 2012.

[52] Laurens Hobert, Andreas Festag, Ignacio Llatser, Luciano Altomare, Filippo Visintainer, and Andras Kovacs. Enhancements of v2x communication in support of cooperative autonomous driving. *IEEE Communications Magazine*, 53(12):64–70, 2015.

[53] Daniel Howard and Danielle Dai. Public perceptions of self-driving cars: The case of berkeley, california. In *Transportation Research Board 93rd Annual Meeting*, volume 14, pages 1–16, 2014.

[54] Ya-Hsin Hung, Robert W. Proctor, Yunfeng Chen, Jiansong Zhang, and Yiheng Feng. Drivers' knowledge of and preferences for connected and automated vehicles. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, volume 66, pages 1457–1461. SAGE Publications Sage CA: Los Angeles, CA, 2022.

[55] Timo Jakobi, Fatemeh Alizadeh, Martin Marburger, and Gunnar Stevens. A consumer perspective on privacy risk awareness of connected car data use. In *Mensch und Computer 2021*, pages 294–302. ACM, 2021.

[56] Timo Jakobi, Gunnar Stevens, Nico Castelli, Corinna Ogonowski, Florian Schaub, Nils Vindice, Dave Randall, Peter Tolmie, and Volker Wulf. Evolving needs in iot control and accountability: A longitudinal study on smart home intelligibility. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 2(4):1–28, 2018.

[57] Ruogu Kang, Stephanie Brown, Laura Dabbish, and Sara Kiesler. Privacy attitudes of mechanical turk workers and the us public. In *10th Symposium On Usable Privacy and Security ({SOUPS} 2014)*, pages 37–49, 2014.

[58] Nico A Kaptein, Jan Theeuwes, and Richard Van Der Horst. Driving simulator validity: Some considerations. *Transportation Research Record*, 1550(1):30–36, 1996.

[59] Christos Katrakazas, Athanasios Theofilatos, George Papastefanatos, Jérôme Härri, and Constantinos Antoniou. Cyber security and its impact on cav safety: Overview, policy needs and challenges. *Advances in Transport Policy and Planning*, 5:73–94, 2020.

[60] Ryan Kennedy, Scott Clifford, Tyler Burleigh, Philip D Waggoner, Ryan Jewell, and Nicholas JG Winter. The shape of and solutions to the mturk quality crisis. *Political Science Research and Methods*, 8(4):614–629, 2020.

[61] John B Kenney. Dedicated short-range communications (dsrc) standards in the united states. *Proceedings of the IEEE*, 99(7):1162–1182, 2011.

[62] Kishwer Abdul Khaliq, Omer Chughtai, Abdullah Shahwani, Amir Qayyum, and Jürgen Pannek. Road accidents detection, data collection and data analysis using v2x communication and edge/cloud computing. *Electronics*, 8(8), 2019.

[63] Ioannis Krontiris, Thanassis Giannetsos, Peter Schoo, and Frank Kargl. *Buckle-up: autonomous vehicles could face privacy bumps in the road ahead*. Ruhr-Universität Bochum, 2020.

[64] J Richard Landis and Gary G Koch. The measurement of observer agreement for categorical data. *Biometrics*, pages 159–174, 1977.

[65] Long Le, Andreas Festag, Roberto Baldessari, and Wenhui Zhang. V2x communication and intersection safety. In *Advanced Microsystems for Automotive Applications 2009*, pages 97–107. Springer, 2009.

[66] Chaiwoo Lee, Carley Ward, Martina Raue, Lisa D'Ambrosio, and Joseph F Coughlin. Age differences in acceptance of self-driving cars: A survey of perceptions and attitudes. In *International Conference on Human Aspects of IT for the Aged Population*, pages 3–13. Springer, 2017.

[67] Hosub Lee and Alfred Kobsa. Confident privacy decision-making in iot environments. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 27(1):1–39, 2019.

[68] Jialiu Lin, Shahriyar Amini, Jason I Hong, Norman Sadeh, Janne Lindqvist, and Joy Zhang. Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, pages 501–510, 2012.

[69] Todd Litman. Autonomous vehicle implementation predictions: Implications for transport planning. https://www.vtpi.org/avip.pdf, 2020.

[70] Jun Liu and Asad J Khattak. Delivering improved alerts, warnings, and control assistance using basic safety messages transmitted between connected vehicles. *Transportation Research Part C: Emerging Technologies*, 68:83–100, 2016.

[71] Na Liu, Alexandros Nikitas, and Simon Parkinson. Exploring expert perceptions about the cyber security and privacy of connected and autonomous vehicles: A thematic analysis approach. *Transportation Research Part F: Traffic Psychology and Behaviour*, 75:66–86, 2020.

[72] Zhaojun Lu, Gang Qu, and Zhenglin Liu. A survey on recent advances in vehicular network security, trust, and privacy. *IEEE Transactions on Intelligent Transportation Systems*, 20(2):760–776, 2018.

[73] Zachary MacHardy, Ashiq Khan, Kazuaki Obana, and Shigeru Iwashina. V2x access technologies: Regulation, research, and remaining challenges. *IEEE Communications Surveys & Tutorials*, 20:1858–1877, 2018.

[74] Naresh K Malhotra, Sung S Kim, and James Agarwal. Internet users' information privacy concerns (iuipc): The construct, the scale, and a causal model. *Information Systems Research*, 15(4):336–355, 2004.

[75] Valerian Mannoni, Vincent Berg, Stefania Sesia, and Eric Perraud. A comparison of the v2x communication systems: Its-g5 and c-v2x. In *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*, pages 1–5. IEEE, 2019.

[76] Davit Marikyan, Savvas Papagiannidis, and Eleftherios Alamanos. A systematic review of the smart home literature: A user perspective. *Technological Forecasting and Social Change*, 138:139–154, 2019.

[77] Lars Müller, Malte Risto, and Colleen Emmenegger. The social behavior of autonomous vehicles. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct*, pages 686–689, 2016.

[78] Kobbi Nissim and Alexandra Wood. Is privacy privacy? *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 376(2128):20170358, 2018.

[79] Patricia A Norberg, Daniel R Horne, and David A Horne. The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, 41(1):100–126, 2007.

[80] Geoff Norman. Likert scales, levels of measurement and the "laws" of statistics. *Advances in health sciences education*, 15(5):625–632, 2010.

[81] Jonathan Petit, Florian Schaub, Michael Feiri, and Frank Kargl. Pseudonym schemes in vehicular networks: A survey. *IEEE Communications Surveys & Tutorials*, 17(1):228–255, 2014.

[82] Minh Pham and Kaiqi Xiong. A survey on security attacks and defense techniques for connected and autonomous vehicles. *Computers & Security*, 109:102269, 2021.

[83] Stefanie Pötzsch. Privacy awareness: A means to solve the privacy paradox? In *IFIP Summer School on the Future of Identity in the Information Society*, pages 226–236. Springer, 2008.

[84] Prashanth Rajivan and Jean Camp. Influence of privacy attitude and privacy cue framing on android app choices. In *Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016)*, 2016.

[85] Joel R Reidenberg, N Cameron Russell, Alexander J Callen, Sophia Qasir, and Thomas B Norton. Privacy harms and the effectiveness of the notice and choice framework. *ISJLP*, 11:485, 2015.

[86] Alejandro Antonio Andrade Salazar, Patrick Drew McDaniel, Ryan Sheatsley, and Jonathan Petit. Physics-based misbehavior detection system for v2x communications. *SAE International Journal of Connected and Automated Vehicles*, 5(3), 2022.

[87] Florian Schaub, Frank Kargl, Zhendong Ma, and Michael Weber. V-tokens for conditional pseudonymity in vanets. In *2010 IEEE Wireless Communication and Networking Conference*, pages 1–6. IEEE, 2010.

[88] Ron Schneiderman. Car makers see opportunities in infotainment, driver-assistance systems [special reports]. *IEEE Signal Processing Magazine*, 30(1):11–15, 2012.

[89] Björn Schünemann. V2x simulation runtime infrastructure vsimrti: An assessment tool to design smart traffic management systems. *Computer Networks*, 55(14):3189–3198, 2011.

[90] Xiaotong Shen, Zhuang Jie Chong, Scott Pendleton, Wei Liu, Baoxing Qin, James Guo Ming Fu, and Marcelo H. Ang. Multi-vehicle motion coordination using v2v communication. *2015 IEEE Intelligent Vehicles Symposium (IV)*, pages 1334–1341, 2015.

[91] Herbert A Simon. Bounded rationality. In *Utility and probability*, pages 15–18. Springer, 1990.

[92] Concas Sisinnio, Kourtellis Achilleas, Karmarani Mohsen, and Dokur Omkar. Connected vehicle pilot deployment program performance measurement and evaluartion-tampa (thea) cv pilot phase 3 evaluation report. https://rosap.ntl.bts.gov/view/dot/55818, 2021.

[93] Manya Sleeper, Sebastian Schnorf, Brian Kemler, and Sunny Consolvo. Attitudes toward vehicle-based sensing and recording. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, pages 1017–1028, 2015.

[94] Daniel J Solove. Introduction: Privacy self-management and the consent dilemma. *Harv. L. Rev.*, 126:1880, 2012.

[95] Carlos Renato Storck and Fátima Duarte-Figueiredo. A 5g v2x ecosystem providing internet of vehicles. *Sensors*, 19(3), 2019.

[96] Gail M Sullivan and Anthony R Artino Jr. Analyzing and interpreting data from likert-type scales. *Journal of Graduate Medical Education*, 5(4):541–542, 2013.

[97] Madiha Tabassum, Tomasz Kosinski, and Heather Richter Lipford. "I don't own the data": End user perceptions of smart home device data practices and risks. In *Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019)*, 2019.

[98] Nazanin Takbiri, Amir Houmansadr, Dennis L Goeckel, and Hossein Pishro-Nik. Limits of location privacy under anonymization and obfuscation. In *2017 IEEE International Symposium on Information Theory (ISIT)*, pages 764–768. IEEE, 2017.

[99] Endel Tulving and Daniel L Schacter. Priming and human memory systems. *Science*, 247(4940):301–306, 1990.

[100] Iis P Tussyadiah, Florian J Zach, and Jianxi Wang. Attitudes toward autonomous on demand mobility system: The case of self-driving taxi. In *Information and communication technologies in tourism 2017*, pages 755–766. Springer, 2017.

[101] National Highway Traffic Safety Administration, U.S. Department of Transportation. Vehicle-to-vehicle communication. https://www.nhtsa.gov/technology-innovation/vehicle-vehicle-communication.

[102] Office of Operations Research and Development, U.S. Department of Transportation. Speed harmonization. https://www.fhwa.dot.gov/publications/research/operations/15012/15012.pdf, 2014.

[103] Björn Wiedersheim, Zhendong Ma, Frank Kargl, and Panos Papadimitratos. Privacy in inter-vehicular networks: Why simple pseudonym change is not enough. In *2010 Seventh International Conference on Wireless On-demand Network Systems and Services (WONS)*, pages 176–183. IEEE, 2010.

[104] Michael S Wogalter. Communication-human information processing (c-hip) model. *Handbook of warnings*, pages 51–61, 2006.

[105] Yong Xi, Kewei Sha, Weisong Shi, Loren Schwiebert, and Tao Zhang. Enforcing privacy using symmetric random key-set in vehicular networks. In *Eighth International Symposium on Autonomous Decentralized Systems (ISADS'07)*, pages 344–351. IEEE, 2007.

[106] Qualtrics XM. Qualtrics. https://www.qualtrics.com/support/website-app-feedback/intercepts-tab/edit-intercept-section/action-set-logic/user-info-conditions/#DeviceType, 2022.

[107] Ziyi Zhang, Shuofei Zhu, Jaron Mink, Aiping Xiong, Linhai Song, and Gang Wang. Beyond bot detection: Combating fraudulent online survey takers. In *Proceedings of the ACM Web Conference 2022*, pages 699–709, 2022.

A APPENDIX

A.1 Scenarios for Privacy Decision-Making

In this appendix, we list the textual descriptions and factor values of all scenarios (S).

S01. An **in-car gaming system** that is connected to the infotainment system shares and receives the **destination and trip details** to **pair you with passengers in nearby vehicles** for online co-op video games.

S02. A **car parking system** installed on your vehicle **sends the data of your vehicle (size, color, license plate, etc.)** to local parking lots and **receives recommendations/locations of parking spaces** from the parking lot.

S03. An **in-car video streaming system** shares the **network conditions and sends requests** to the remote data center and **receives the videos** in-demand.

S04. The **trip planning system** installed on your vehicle helps you find **facilities (such as gas stations)** nearby by **collecting your location, vehicle statistics, and payment information** and **receiving information about services offered and the prices**.

S05. The **trip planning system** installed on your vehicle **sends your location and upcoming trip details** and **receives timely updates on detours and planned events** from the local transportation management center to **avoid road closings and congestion**.

S06. The **trip planning system** installed on your vehicle **shares the vehicle information (such as the location, height, width, types of tires)** with the roadside infrastructure data system and **receives warnings about the road conditions** such as the vertical clearance and dynamic weather update to **plan a safe route**.

S07. The **trip planning system** installed on your vehicle **shares its location and speed at highway on-ramps and off-ramps** with the roadside unit to help **improve the road traffic control**. Meanwhile, it **receives the recommended optimal speed** from the roadside unit to **avoid congestion**.

S08. The **navigation system** installed on your vehicle **shares its speed, heading, and vehicle type** and **receives the same information from nearby emergency vehicles** to **give the right of way**.

S09. The **autonomous sensing system** installed on your vehicle **detects and analyzes the movements of pedestrians** around you to **infer unusual behaviors**. The vehicle may **send a warning** to other vehicles if it detects unlawful pedestrian crossings. It may also **receive warnings from other vehicles**.

S10. The **intersection movement assist system** installed on your vehicle **shares and receives the speed, location, heading, brake status, steering wheel angle, and path prediction** with adjoining vehicles before entering the intersection to **avoid sideswipe collisions**.

S11. The **traffic navigation system** installed on your vehicle helps other vehicles near you to be prepared by **broadcasting your CAV's lane changes, acceleration, and deceleration** in advance. The vehicle also **receives lane changes, acceleration, and deceleration of other vehicles** to **avoid collisions**.

S12. The **in-vehicle safety and emergency monitoring system** shares the **status (such as tire pressure, windshield, brake) of your vehicle** to nearby roadside assistance so that **timely help and rescue can be received and deployed**.

S13. The **autonomous sensing system** installed on your vehicle helps avoid collision with other vehicles near you by **sharing and receiving real-time GPS coordinates** to **improve safety**.

S14. The **autonomous sensing system** installed on your vehicle **takes pictures of the surroundings** with its 360° coverage camera suite to **recognize vehicles, pedestrians, and objects** and **share this information** with other vehicles to **improve safety**. It also **receives pictures taken by other vehicles and the roadside unit** for a **collaborative perception**.

S15. The **autonomous sensing system** installed on your vehicle **scans the environment** with laser beams emitted from LiDAR sensors to **detect approaching vehicles, pedestrians, and objects** and **share this information** with other vehicles to **improve safety**. It also **receives LiDAR data** collected by other vehicles and the roadside unit to **work collaboratively**.

S16. The **autonomous sensing system** installed on your vehicle **shares and receives the movement of the environment (such as the velocity, and depth)** detected by the radar sensor with nearby vehicles and roadside units.

A.2 Tables

Table 4 shows the results of all measures (perceived benefits and perceived risks of sharing data and receiving data, data-sharing willingness and confidence ratings). Previous literature showed that parametric tests such as ANOVA are sufficiently robust to yield the correct answer even when distributional assumptions are violated [80] (e.g., likert scale responses [96]). Thus, we also built a linear mixed-effects regression (or LMER) for each model with the lme4 package in R [11]. Table 5 shows the results of ANOVA and the post-hoc analysis that provides pairwise comparisons beyond the comparisons with baseline in Regression analysis. There were significant main effects of *scenario* in perceived benefits, perceived risks and data-sharing decisions, and *condition* in perceived benefits and data-sharing decisions. Thus, we obtained consistent results by using LMER and CLMM, in agreement with results in the literature (e.g., [18]).

Table 4: **Results of Four Measures of Sharing Data and Two Measures of Receiving Data in Phase 2 as a Function of Scenario and Condition.** The number in the parentheses of the first column indicates the number of participants in each condition. The number in the parentheses of the last three columns shows the standard errors of corresponding cell.

Sharing Data

Condition	Scenario	Benefit	Risk	Willingness	Confidence
Control (220)	Infotainment	4.54 (0.13)	4.76 (0.12)	4.24 (0.14)	5.64 (0.09)
	Traffic management	5.65 (0.10)	4.30 (0.13)	5.40 (0.11)	5.82 (0.07)
	Road safety	5.95 (0.10)	3.99 (0.14)	5.68 (0.11)	5.87 (0.08)
	Autonomous driving	5.90 (0.10)	4.21 (0.13)	5.56 (0.11)	5.78 (0.08)
Privacy priming (202)	Infotainment	4.02 (0.14)	5.25 (0.12)	3.78 (0.14)	5.69 (0.09)
	Traffic management	5.46 (0.11)	4.50 (0.13)	5.13 (0.12)	5.89 (0.08)
	Road safety	5.69 (0.10)	4.12 (0.14)	5.42 (0.11)	5.99 (0.08)
	Autonomous driving	5.48 (0.10)	4.49 (0.14)	5.24 (0.11)	5.67 (0.09)
Privacy&security priming (173)	Infotainment	4.21 (0.15)	5.10 (0.13)	3.80 (0.15)	5.60 (0.10)
	Traffic management	5.79 (0.12)	4.34 (0.15)	5.29 (0.13)	5.73 (0.08)
	Road safety	5.64 (0.11)	4.20 (0.15)	5.28 (0.12)	5.60 (0.09)
	Autonomous driving	5.52 (0.11)	4.34 (0.15)	5.08 (0.12)	5.59 (0.09)

Receiving Data

Condition	Scenario	Benefit	Risk
Privacy&security priming (173)	Infotainment	4.50 (0.08)	4.75 (0.07)
	Traffic management	5.86 (0.05)	4.00 (0.08)
	Road safety	5.75 (0.06)	3.95 (0.08)
	Autonomous driving	5.73 (0.06)	4.09 (0.07)

Table 5: **Effects of Condition and Scenario on Four Measures at Phase 2.** We build each LMER model by considering the two main effects and their interaction and report F and p values. We report DoF with Satterthwaite denominator degrees of freedom. Post-hoc pairwise comparisons are conducted when needed. Significance is denoted by *** ($p < 0.001$), ** ($p < 0.01$), and * ($p < 0.05$).

Factor	Perceived Benefits			Perceived Risks			Willingness			Confidence		
	DoF	***F***	***p***	**DoF**	***F***	***p***	**DoF**	***F***	***p***	**DoF**	***F***	***p***
Condition	(2, 592.72)	4.16	.016*	(2, 591.67)	1.81	.164	(2, 591.84)	4.06	.018*	(2, 592.05)	2.41	.090
Con. vs. Pri.			.014*						.053			
Con. vs. Pri.+Sec.	N/A	N/A	.248	N/A	N/A	N/A	N/A	N/A	.039*	N/A	N/A	N/A
Pri. vs. Pri.+Sec.			.996						1			
Scenario	(3, 11.74)	12.95	<.001***	(3, 11.00)	10.19	.002**	(3, 11.67)	13.93	<.001***	(3, 9.58)	2.88	.091
Info. vs. Traff.			.002**			.019*			.002**			
Info. vs. Safety			.001**			.002**			<.001***			
Info. vs. Auto.	N/A	N/A	.002**	N/A	N/A	.015*	N/A	N/A	.002**	N/A	N/A	N/A
Traff. vs. Safety			1			1			1			
Traff. vs. Auto.			1			1			1			
Safety vs. Auto.			1			1			1			
Condition * Scenario	(6, 1767.03)	2.02	.060	(6, 1787.67)	0.90	.495	(6, 1765.94)	1.17	.317	(6, 1772.97)	1.35	.230