Perceived Risks toward In-Vehicle Infotainment Data Services on Intelligent Connected Vehicles

Zhiyuan Yu * and Kexin Cai

School of Journalism and Communication, Shandong University, Jinan 250100, China
* Correspondence: yuzhiyuan@sdu.edu.cn

Abstract: With the evolution of Internet of Vehicles (IoV) and intelligent transportation systems, intelligent connected vehicles (ICV) are becoming the trend in automobile industry worldwide. Assisted by road-side infrastructure and vehicle-mounted sensors, in-vehicle infotainment (IVI) data services are gradually growing more popular with drivers and passengers. In particular, IVI data services are not only restricted to internal cabin, but also are being extended to the external environment (e.g., workplace and home). These data categories include personal demographics/bioinformatics, usage habits, travel patterns, real-time location, audio, video, etc., which in turn induce perceived risk concerns around the data privacy and security of occupants. In this paper, we collect answers from 500 valid respondents and then construct a structural equation model to investigate key factors influencing users’ attitudes and behavioral intention (BI) towards IVI data services. Therein, trust is considered to play a vital role in attitude, and is assumed to be affected by perceived security risk (PSR), perceived privacy risk (PPR), and perceived performance risk (PFR). The results show that PSR and PPR have negative effects on user trust. The data breach anxiety positively influences PPR, which explain 75% of variance. In addition, trust can directly affect attitude and BI, which explain 28.6% of variance in attitudes towards IVI data services. Respondents score higher on average for attitude (Mean = 5.762, SD = 0.89) even where perceived risks exist. BI is influenced by the factors of PSR, PFR, trust, and attitude. Through this study, we intend to reveal the relationships among the factors of perceived risk, trust, attitude, and BI towards IVI data services, then provide guidelines for vehicular data governance in order to consolidate user trust for a safer mobility ecosystem.

Keywords: data services; intelligent connected vehicles; in-vehicle infotainment; perceived privacy and security risks; trust

1. Introduction

With the emerging trend in automobile industry, intelligent connected vehicles (ICV) are becoming giant mobile systems consisting of artificial intelligence technology and smart hardware equipment, which support the functions of infotainment, environmental awareness, decision-making, and motion control [1]. According to Statista reporting, the number of connected cars was expected to reach 236.54 million in 2021 and increase to 863.17 million worldwide by 2035 [2]. Supported by Internet of Vehicle (IoV) and sensor-based devices (as shown in Appendix A Table A1), ICV can be turned into massive data hubs [3] and combine a large number of different in-vehicle infotainment (IVI) data services, including telematics and driving assistance (e.g., fleet management, remote control, rear-view cameras, navigation, etc.), entertainment (e.g., streaming media, online podcasts, video-on-demand, gaming, etc.), intra-vehicular applications (home–car connections, messaging, social media, etc.). The data types involved in ICV include user information (e.g., trajectory, portrait, biometric authentication), geographic information, human/vehicle flow, etc. In order to improve the quality of personalized experience, automakers, original equipment manufacture (OEM), and service providers (SP) all inevitably need to collect, analyze, and process data related to drivers and passengers. This raises users’ concerns about the disclosure or abuse.
of private information. In this way, data privacy and security risks in the ICV context have attracted a great deal of attention.

General Data Protection Regulation (GDPR) is a popular and widely accepted data controller which can provide a privacy and data protection impact assessment to guarantee personal data rights such as access, recording, processing, being informed, being forgotten, etc. [4]. In order to obtain efficient services and social benefits, the UK Information Commissioner Office requires that the risks of data sharing be assessed and mitigated [5]. Through the vulnerabilities of vehicle-mounted applications, hackers could access vehicle control systems, leading to unexpected accidents via remote operation (e.g., braking or acceleration). Moreover, as more connections are established among workplace, home, and ICV by IoV, the potential scope of loss is enlarged via the intermediate nodes. Meanwhile personal profiles of drivers and passengers can be leaked when security systems are attacked. In the U.S., the Self-Driving Act mentions that high-level automated vehicle manufacturers must prioritize cybersecurity and develop a privacy plan with respect to data collection, usage, sharing, and storage for both owners or occupants [6]. In China, the Ministry of Industry and Information Technology highlights IoV-based data security and has put forward measures to prevent data leakage, damage, loss, tampering, misuse, and abuse [7]. In Europe, personal data transfer policy is restricted among vehicle manufacturer, SP, or other data controllers [3]. To deal with these numerous ICV performance risk challenges, the U.S. [8], Australia [9], and China [10] all require installation of in-vehicle Event Data Recorders (EDR) to monitor different types of vehicle-mounted devices. In addition, imperfect conditions such as light reflection and image scanning may cause uncertainty that can affect decision results, potentially even causing system failure or incorrect behavior [11].

Considering that vehicle-mounted data services (e.g., driving route and positional tracking) are relatively sensitive, improper use causes potential risks to privacy, security, and performance for both drivers and passengers. In addition, ICV are not fully popularized and customers may lack relevant knowledge, making it easy to distrust or doubt the data services provided in ICVs. Therefore, it is necessary to study the perception of perceived risk towards data services and then explore the degree of trust involved in human–machine interaction. Therefore, in this paper we aim to discover the factors influencing user attitudes and behavioral intentions (BI) in term of ICV data services, which can lead to establishing or improving user trust and acceptance of added-value data services. On this basis, we aim to solve the following research questions (RQ):

- RQ 1: What is the relationship between users’ perceived risk and trust in IVI data services of ICV?
- RQ 2: How do relevant factors affect users’ attitudes and BI towards IVI data services in ICVs?

The structure of this paper is as follows. The theoretical background related to human attitudes and behaviors is introduced in Section 2. The theoretical model and proposed hypotheses are presented in Section 3. Section 4 describes the demographic characteristic and the results of data analysis. Section 5 reveals the main findings and points out the implications and limitations of this study. Finally, Section 6 concludes this paper.

2. Literature Review
2.1. Theoretical Background

A series of theoretical models attempt to explain and predict the complexity of human behavior, e.g., Theory of Reasoned Action (TRA), Theory of Planned Behavior (TPB), Technology Acceptance Model (TAM), Unified Theory of Acceptance and Use of Technology (UTAUT), etc. Among these, TRA is regarded as the most influential theory of human cognitive behavior; it assumes that human beings are rational, considering various kinds of information and preferring to choose to maximize their own interests before carrying out behaviors [12]. TRA states that behavioral intention (BI) determines individual behavior, which in turn is influenced by attitude and subjective norms. TRA has a wide range
of applications, including catering [13–15], science and technology [16–18], and life and health [19–21]. Due to the openness of TRA, new variables are often included in the extended study of the theory, such as Theory of Planned Behavior.

TPB is a fundamental theory in the study of human decision-making in social psychology; it reveals that human behavior is directly influenced by BI, while BI is in turn affected by the factors of attitude, subjective norms, and perceived behavioral control [22]. Compared with TRA, TPB can eliminate limitations in dealing with behavior involving incomplete volitional control [23]. Currently, TPB and its extended model are widely applied in research fields in transportation [24], healthcare [25,26], information technology [27,28], and environmental science [29,30], where it has been successful in explaining and predicting personal usage behavior. BI refers to an individual’s preparation or intention to engage in a specific behavior. Attitude, subjective norms, and perceptual behavioral control strengthen an individual’s BI. Attitude is an individual’s subjective evaluation of a particular behavior. A favorable or unfavorable attitude directly affects an individual’s BI. Subjective norms represent the organizational or social pressure a person feels to implement them. Perceived behavioral control refers to the degree of difficulty that an individual perceives when performing a behavior. Generally speaking, the more favorable an individual’s attitude and subjective norms towards a behavior are, the stronger that individual’s willingness to carry out the behavior is [22].

2.2. Perceived Risk Research in ICV-Related Field

With the evolution of intelligent transportation systems (ITS) and telematics, IVI and its application have become the standard ICV configuration, providing data services to improve the experience of drivers and passengers. Although IVI with online data services provide a great deal of convenience, users may be concerned about potential risks when using ICV data services. For example, ICVs share data through and with the internet or other smart devices. This poses a security threat, as ICVs can be affected by factors such as in-car hacking, malware tampering with data, and even remote control [31].

Perceived risk is gradually being recognized as the vital factor guaranteeing traffic safety when using driving assistance and IVI applications, as consumers consider both incentives and threats in their adoption decisions [32]. Jacoby et al. have proposed seven types of risk: financial risk, performance risk, physical risk, psychological risk, and social risk [33], with Roselius taking an additional dimension of temporal risk into account [34]. Bhatnagar et al. have suggested that information security risk is one of the most important risks in the context of online shopping [35]. Featherman et al. divided perceived risk into seven dimensions: performance, financial, time, psychological, social, privacy, and overall risk, and pointed out that the intensity of perceived risk varies with the services involved [36]. Therein, the main findings in ICV-related field are summarized in Table 1 and presented as follows:

- **ITS:** Miltgen et al. found that perceived risk reduces users’ willingness to accept biometric systems and that more privacy-conscious consumers perceive greater risk [37]. Vandeza et al. proposed that monitoring and tracking of vehicles, data collection, storage, and other processes lead to many different privacy risks in ITS [38]. In a study of electronic speed detectors, Marell et al. confirmed that automobile traffic contains a variety of risk factors, including accident risk, public risk, personal risk, and environmental risk, and found that drivers tend to accept electronic speed detectors as a way to reduce traffic risk [39].

- **Telematics:** Kim et al. confirmed that perceived risk has a positive effect on user resistance to acceptance of IVI systems [40]. Maeng et al. found that compared with remote carjacking, consumers are more alert and vigilant to communication failures and unauthorized collection of personal information [41]. Walter et al. found that privacy risk was one of the most important perceived risks involving data services in connected vehicles and that it had a significant negative impact on attitudes [42].
• Autonomous Vehicles: Wu et al. found that individuals’ views on the perceived risks of autonomous buses had a significant detrimental effect on trust [43]. Lee et al. demonstrated that perceived risk negatively affects users’ willingness to use an autonomous vehicle [44]. Kapser et al. found a significant negative correlation between perceived risk and the behavioral intentions of relying on automatic delivery vehicles [45].

With the assistance of vehicle-mounted sensors (e.g., radar, cameras) and IoV, ICVs can function as a giant mobile system to provide basic data services and realize inter-operational data sharing. As they are a common issue in Internet of Things (IoT) scenarios [46], vulnerabilities (e.g., hacking, behavior monitoring) have made users suspicious and distrustful of ICV data services. At present, there are few studies on the technical acceptability of data services in the context of privacy security in ICVs. Therefore, it is necessary to conduct quantitative research in order to predict users’ attitudes and BI. In light of the above, the contributions of this paper can be summarized as follows:

• Based on the theory of planned behavior and theory of reasoned action, we propose a structural equation model to explore the risk perceived by users of data services in ICVs and reveal their attitudes and behavioral intentions.

• We refine the perceived risks of IVI data services into three constructs, namely, perceived security risk (PSR), perceived privacy risk (PPR), and perceived performance risk (PFR), in order to respectively reveal their relationships with trust according to characteristics of ICVs. Herein, we find that data breach anxiety is a vital factors for perceived privacy risk.

• Despite the perceived risks involved, the respondents show high attitude and behavioral intention to use in-vehicle infotainment data services. We find that PSR reduces user trust and BI, PPR has a negative effect on trust, and DBA aggravates PPR.

Table 1. Overview of research findings.

| Subject and Source | Research Findings |
|--------------------|-------------------|
| ITS [37]           | Perceived usefulness (PU) → BI  |
|                    | Compatibility (C) → BI |
|                    | Facilitate conditions (FC) → BI |
|                    | Perceived risks (PR) → BI  |
|                    | Trust in technology (TT) → BI |
|                    | Innovativeness (Innov) → BI  |
|                    | Privacy concerns (PC) → Perceived risks (PR) |
|                    | BI → Recommendation (REC)    |
| IVI systems [40]   | Perceived risk (PR) → Resistance (RS) |
|                    | RS → Intention to use (IU)   |
|                    | Technographics (TG) → Perceived usefulness (PU) |
|                    | TG → Perceived complexity (PC) |
|                    | TG → PR                      |
|                    | PU → RS                      |
|                    | PC → RS                      |
|                    | Subjective norms (SN) → PU   |
|                    | SN → PR                      |
| Automotive telematics [42] | Perceived usefulness (PU) → ATT |
|                    | Perceived ease of use (PEOU) → PU |
|                    | ATT → Behavioral Intention (UI) |
|                    | Privacy Concerns (PC) → Perceived Risk (PR) |
|                    | PC → Trust in Provider (TR)  |
|                    | PR → ATT                     |
|                    | Information Control (IC) → PC |
|                    | SN → UI                      |
Table 1. Cont.

| Subject and Source | Research Findings                          |
|--------------------|-------------------------------------------|
| Autonomous Vehicles [47] | Performance Expectancy → Adoption  
Reliability → Trust  
Security → Trust  
Privacy → Trust  
Trust → Adoption |

3. Research Model and Hypotheses

In this study, a modified theory of planned behavior and theory of reasoned action model is proposed to investigate user attitudes and behavioral intentions towards ICV data services. We designed a structural equation model (SEM) integrating the constructs of trust, perceived security risk (PSR), perceived privacy risk (PPR), perceived performance risk (PFR), and data breach anxiety (DBA) with attitude (ATT) and behavioral intention (BI), which these terms are defined in Table 2. Following previous studies, we first present our theoretical model and then describe the causal relationship between the constructs.

Table 2. Definition of constructs.

| Construct | Definition                                                                 | Reference                                      |
|-----------|---------------------------------------------------------------------------|-----------------------------------------------|
| PSR       | The degree to which ICV drivers or passengers are concerned about security risks when using IVI data services. | Yenisey et al. (2005) [48]                    |
| PPR       | The degree to which ICV drivers or passengers envisage potential loss of personal privacy when using IVI data services. | Jarvenpaa and Todd (1996) [49]                |
| PFR       | The possibility that IVI data services in ICVs may not perform as well as expected in data security and privacy protection or fail to provide the desired benefit. | Grewal et al. (1994) [50]                     |
| DBA       | The perceived stress or anxiety associated with hacking or electronic data breaches. | Elhai and Hall (2016) [51]                    |
| Trust     | Users’ general belief in ICV data services providers, resulting in BI.   | Gefen et al. (2003) [52]                      |
| ATT       | The degree to which users perceive positive or negative feelings concerning IVI data services in ICVs. | Wu and Zhang (2014) [53]                     |
| BI        | The subjective probability of drivers or passengers using data-related services in ICVs. | Walter and Abendroth (2020) [42]              |

3.1. Attitude and Behavioral Intention

Individual attitudes have a significant impact on the popularity of new technologies [54], and a positive correlation exists between attitude and individual BI in the adoption of emerging applications or services. For example, Wu et al. [43] have proved that passengers’ attitude towards automatic buses positively affects their BI. Walter et al. [42] have found that users’ attitude towards using online vehicle services has a significant positive impact on BI. Zhang et al. [55] have confirmed that the behavioral intention of users to accept automated vehicles is positively affected by their attitude. Vijayasarathy [56] have found that attitude has a positive impact on willingness to engage in online shopping. Therefore, based on these prior studies we believe that driver and passenger attitudes
toward ICV data services will affect willingness to use and then put forward the following hypothesis:

**Hypothesis 1 (H1).** Individuals’ attitude towards IVI data services in ICV has a positive influence on their behavioral intention.

### 3.2. Trust

The adoption of new technologies involves uncertainty. As with other intelligent devices (e.g., mobile phones or tablets), there exist privacy and security risks (e.g., disclosure and tracking) when using data-related services in ICV. An environment of trust needs to be established between service providers and users to ensure that individuals worry less about uncertainty; this has a positive impact on the adoption of new technologies [57]. Yang et al. [58] showed that users’ trust in smart home service providers is an important factor influencing their attitudes. Zhang et al. [55] found that trust has a positive impact on attitudes towards the use of automated vehicles. Jarvenpaa et al. [59] demonstrated that consumer trust in internet stores positively influences attitudes toward online shopping. Therefore, the following hypothesis is proposed:

**Hypothesis 2a (H2a).** Individuals’ trust towards IVI data services in ICV has a positive influence on attitudes towards use.

Fang et al. [60] found that trust in the sponsor of a web survey can positively affect potential respondents’ attitudes towards the survey as well as their willingness to participate. Muangmee et al. [61] revealed that perceived trust positively influenced willingness to use food delivery apps during the COVID-19 pandemic. The study of Miltgen et al. [37] confirmed that there is a positive correlation between consumers’ trust in biometric systems and their behavioral intention to accept such systems. Pavlou’s research [62] has found that consumer trust in e-commerce has a positive impact on online transaction intention. We therefore propose the following hypothesis:

**Hypothesis 2b (H2b).** Individuals’ trust towards IVI data services in ICV has a positive influence on behavioral intention to use.

### 3.3. Perceived Security Risk

Users are greatly worried about the risks associated with ICV, and security risks are the most important concern [63]. Security reflects people’s views on data transmission and storage mechanisms [64]. In order to provide better services, ICV can collect large amount of data about users’ travel patterns and driving directions, such as the identity of the owner, their driving trajectory and habits, etc. At the same time, these programs and applications are flawed in terms of security. It has been revealed that potential safety issues caused by hacking are a serious concern for users of autonomous vehicles [65]. Zhang et al. [55] have found that perceived security risk has a negative impact on consumers’ initial trust towards autonomous vehicles. For online purchase of tourism products, Ponte et al. [66] showed that perceived security was the main factor affecting perceived trust. A lack of security protection leads consumers to distrust online shopping. Kaur et al. [47] demonstrated that security safeguards can increase trust in driverless cars. On this basis, we propose the following hypothesis:

**Hypothesis 3a (H3a).** Perceived security risk has a significant negative influence on trust towards IVI data services in ICV.

For online shopping, Kim et al. [67] have confirmed that perceived risks, including security risks, can directly reduce consumers’ willingness to use. Anthony et al. [68] have found that user concerns about the security of online shopping systems decrease online shopping rates. Therefore, the following hypothesis is proposed:
Hypothesis 3b (H3b). Perceived security risk has a significant negative influence on behavioral intention towards IVI data services in ICV.

3.4. Perceived Privacy Risk

In addition to perceived security risks, perceived privacy risks play a vital role in the study of data-related services. During the use of ICV, privacy risks arise from the fact that travel and behavioral data may be transmitted to governments or third-party service providers (e.g., vehicle factory and insurance companies) without users’ authorization. This makes it possible for the third-party service provider to violate users’ data privacy for economic benefit. Moreover, as an intelligent entity, an ICV may be attacked by others, e.g., hackers [55]. Privacy deterioration is considered a major issue for autonomous vehicles, especially in high-income countries [69]. As they are equipped with various kinds of internal sensors and external radars, private data about driver and passenger demographics, real-time location data, travel patterns, plans, and parking or commuting status could be surveilled during use [70]. With respect to privacy issues, studies suggest that the various uses of customers’ personal data leads to the perception of vulnerability, which can prompt customers to respond to companies’ efforts to collect and use their personal data [71].

Bhattacherjee [72] suggested that service providers should allow users to choose how personal information is used, which is an important measure of trust. Metzger’s research [73] confirmed that concerns about online privacy can have a negative impact on users’ trust in commercial websites. Thus, we assume the following:

Hypothesis 4 (H4). Perceived privacy risk has a significant negative influence on trust towards IVI data services in ICV.

3.5. Perceived Performance Risk

Perceived performance risk is a part of PR [74] and has been shown to be perceived by internet users [75]. Cunningham [76] assumed that all risk levels were derived from performance risk, which consists of economic, time, and effort performances. In addition to safety risks, Kapser et al. [45] revealed that self-driving cars present performance risks due to technical glitches. When drivers and passengers face data service barriers and lack of protective measures, and when performance does not match expectations, this increases the perceived performance risk. Bhattacherjee [77] found that service providers should allow users to choose how personal information is used, which is an important measure of trust. George et al. [78] confirmed that the existence of perceived risks (including performance risks) reduces user trust in online shopping providers. Therefore, we assume the following:

Hypothesis 5a (H5a). Perceived performance risk has a significant negative influence on trust towards IVI data services in ICV.

Littler et al. [79] have found that failures of internet banking reduce user engagement. Forsythe et al. [80] have revealed that perceived risk of poor product performance in online shopping is negatively correlated with purchase intention. The performance risk of buying clothes online affects the purchasing intentions of users [81]. Lee et al. [82] have confirmed that perceived risks associated with online retailers negatively affect the attitudes and behaviors of online consumers. Therefore, the following hypotheses are proposed:

Hypothesis 5b (H5b). Perceived performance risk has a significant negative influence on attitude towards IVI data services in ICV.

Hypothesis 5c (H5c). Perceived performance risk has a significant negative influence on behavioral intention towards IVI data services in ICV.
3.6. Data Breach Anxiety

Technological anxiety represents the emotional state of anxiety or fear generated by users when using innovative technological products [83]. As confirmed by Elhai et al. [51], this anxiety is universal regardless of socio-economic status. Meuter et al. [84] have suggested that technology anxiety is one of the most important psychological antecedents affecting users’ adoption of new technologies. Dinev et al. [85] have confirmed that there is a close correlation between perceived vulnerability and privacy concerns, with internet users gradually becoming aware of the power of internet-based technologies to gather information without their knowledge. Considering data-related services for ICV, we interpret technical anxiety as data breach anxiety. Elhai et al. [51] have compiled a list of ten possible hacking security breaches, such as instant messages being intercepted, cloud storage being hacked, and passwords being stolen from social media and internet accounts; they call the concerns and stresses associated with cybersecurity, hacking, and data breaches “electronic data breach anxiety”. Solove et al. [86] have pointed out through a study of relevant court cases that data breaches can cause intangible harm and risk and create anxiety for users, which should be taken seriously. Chakraborty et al. [87] have found that data leakage caused by hacking events is an important driver of users’ perceived risk during online shopping. Due to concerns about data privacy, users are likely to feel fear and anxiety about data leaks from ICV. Therefore, we propose the following hypothesis:

**Hypothesis 6 (H6).** Data breach anxiety has a significant positive influence on perceived privacy risk towards IVI data services in ICV.

Figure 1 shows the proposed theoretical model along with the above hypotheses.

![Figure 1. The proposed theoretical model.](image)

4. Results of Data Analysis

4.1. Data Collection and Demographic Characteristics

We conducted an online questionnaire survey through a survey platform and social media from 25 April to 16 May 2022. For respondents in the online survey, we only recruited those who had experience with data services in ICV, which was ensured via setting a filtering question (i.e., filling car mode, data service type, or application). Based on statistical reports of automobile insurance, the monthly penetration rate of ICV among new cars in the year 2021 varied from about 5% to 18.68%, which are all less than 20% [88]. Although there exist 450 million drivers in China, not all drivers are used to operating or experiencing ICV data services.
On the one hand, we attempted to obtain a larger sample size via survey platforms (Credamo and WJX) in order to break through geographical limitations and expand the collection range of samples. On the other hand, we shared the questionnaire on social media (Wechat and QQ) by snowball sampling. In order to ensure that participants had experienced or used ICV data services, we deleted invalid questionnaires according to the following criteria: (1) those who had not been exposed to ICV data services; and (2) responses with a filling time less than 170 s. On this basis, 500 of 555 questionnaires were ultimately considered as valid. For each item in Appendix B Table A2, a 7-point Likert scale ranging from “strongly disagree = 1” to “strongly agree = 7” was used. At the same time, respondents were asked to rate how often they used IVI while commuting, from “1 = rarely use” to “10 = frequently use”. The average score was relatively high (M = 8.016, SD = 1.491). We analyzed the overall reliability and validity of the questionnaire by SPSS, with the results shown in Table 3. Cronbach’s α coefficient > 0.8 indicates that the reliability is acceptable. The Bartlett test can check the degree of correlation between various variables. KMO > 0.9 indicates strong correlation. With a p value < 0.05, the questionnaire has construct validity. Therefore, the questionnaire has relatively good reliability and validity.

Table 3. Reliability and validity of questionnaire.

| Cronbach’s α | KMO   | p Values |
|--------------|-------|---------|
| 0.898        | 0.961 | 0.000   |

The demographic characteristics of valid respondents are shown in Table 4, with 53.8% being male and 46.2 percent female. According to China’s traffic laws and regulations, the minimum age for applying for a motor vehicle driving license is 18. In terms of age distribution, participants aged 26–35 and 18–25 were dominant, accounting for 53.6% and 22.6%, respectively; 18.2% of respondents were aged 36–45, while 5.6% were over 46. In terms of education, 96.4 percent of the respondents had received higher education, with 70.4 percent at the undergraduate level and 13.6 percent with a Master’s degree and above; 32.6% and 44% of respondents have 3–5 years and more than 5 years driving experience, respectively. According to the group income classification of the National Bureau of Statistics of China, we classified the income status of respondents into four levels, i.e., low income, middle income, considerable income, and high income. Those with a monthly income of less than CNY 2000 (about USD 300) accounted for 3.2%. The middle income group, with a monthly income of CNY 2000–5000 (about USD 300.15–750) accounted for 18.2%, while 49.6% of respondents had a considerable income of CNY 5000–10,000 (about USD 750.15–1500) and 29% of respondents had a high income of more than CNY 10,000 (about USD 1500). Based on self-reported geographical location, 500 valid questionnaires come from 28 provincial-level administrative regions in China, including Shandong, Beijing, Guangdong, Hubei, and Shaanxi. All major economic regions in China have the respondents to fill out the questionnaire, with most of the respondents coming from Eastern, Central, and Western China, accounting for 65.2%, 17% and 12.6%, respectively. The remaining 5.2% were from Northeastern China.
Table 4. Descriptive analysis.

| Profile Category | Number | Percentage |
|------------------|--------|------------|
| **Gender (N = 500)** |        |            |
| Male             | 269    | 53.8       |
| Female           | 231    | 46.2       |
| **Age**          |        |            |
| 18–25            | 113    | 22.6       |
| 26–35            | 268    | 53.6       |
| 36–45            | 91     | 18.2       |
| 46–60            | 28     | 5.6        |
| **Education**    |        |            |
| Junior high and below | 3 | 0.6 |
| High school      | 15     | 3.0        |
| College          | 62     | 12.4       |
| Undergraduate    | 352    | 70.4       |
| Graduate and above | 68 | 13.6      |
| **Driving experience** | | |
| 0 years (with license) | 9 | 1.8 |
| 1–2 years        | 108    | 21.6       |
| 3–5 years        | 163    | 32.6       |
| 6–10 years       | 152    | 30.4       |
| 11–15 years      | 45     | 9.0        |
| 16–20 years      | 16     | 3.2        |
| Over 20 years    | 7      | 1.4        |
| **Income (USD/month)** | | |
| Under 300        | 16     | 3.2        |
| 300.15–450       | 18     | 3.6        |
| 450.15–600       | 24     | 4.8        |
| 600.15–750       | 49     | 9.8        |
| 750.15–900       | 44     | 8.8        |
| 900.15–1050      | 31     | 6.2        |
| 1050.15–1200     | 49     | 9.8        |
| 1200.15–1350     | 53     | 10.6       |
| 1350.15–1500     | 71     | 14.2       |
| Above 1500       | 145    | 29         |
| **Area**         |        |            |
| Northeastern China | 26 | 5.2 |
| Eastern China    | 326    | 65.2       |
| Central of China | 85     | 17.0       |
| Western China    | 63     | 12.6       |

Exchange rate: 1 CNY = 0.15 USD

4.2. Data Analysis and Modeling Results

The partial least squares structural equation model (PLS-SEM) can test the relationship between potential variables and determine the existence of the critical path, which has stronger interpretation and prediction ability [89]. Based on this, PLS-SEM has been widely applied in information systems [90], accounting research [91], tourism [92], and other fields. We used SmartPLS 3.3.3 to evaluate the proposed theoretical model. The PLS algorithm was used to test the measurement model, with a maximum number of iterations of 300 and a stop criterion of $10^{-7}$. To test the structural model, 5000 subsamples were set up with PLS bootstrapping, bias correction and acceleration, and two-tailed hypothesis testing. A blindfold was used to keep the default setting of Level 7 missing distance.

4.2.1. Reliability and Validity Measurement

Internal consistency reliability along with convergent and discriminant validity tests were used to evaluate the measurement model. The internal consistency reliability consists of Cronbach’s $\alpha$ and composite reliability (CR). To assess convergent validity, the indicators of outer loading (>0.70) and average variance extracted (AVE) (>0.50) are used to evaluate
each construct. The variance inflation factor (VIF) evaluates collinearity issues (<5, ideally close and lower than 3) [93,94].

Table 5 shows the outer loading, Cronbach’s α, CR, AVE, and VIF. It can be seen that the reliability of the measurement items is justified. Cronbach’s α and CR range from 0.673 to 0.911 and 0.802 to 0.938, respectively, which indicate that the questionnaire has good internal consistency and high reliability. The ranges of AVE values between 0.504 and 0.790 prove that all constructs passed the test and demonstrate good convergence validity. All values of VIF are lower than 5, and most are less than 3, which is acceptable. According to the Fornell–Larcker criterion, the square root of the AVE of each construct should be greater than the highest correlation with other constructs, meaning that there are connotations and empirical differences between each variable. Table 6 displays the results of the Fornell–Larcker criterion, showing that the square root of AVE (in bold on the diagonal) is higher than the inter-construct correlations (off-diagonal values), verifying the discriminant validity.

Table 5. Reliability and convergent validity.

| Construct | Item | Loading | VIF | Cronbach’s α | CR  | AVE   |
|-----------|------|---------|-----|--------------|-----|-------|
| BI        | BI1  | 0.729   | 1.332 | 0.673        | 0.802 | 0.504 |
|           | BI3  | 0.715   | 1.217 |              |      |       |
|           | BI5  | 0.714   | 1.347 |              |      |       |
|           | BI6  | 0.681   | 1.237 |              |      |       |
| DBA       | DBA1 | 0.859   | 2.817 | 0.903        | 0.932 | 0.774 |
|           | DBA3 | 0.896   | 3.350 |              |      |       |
|           | DBA4 | 0.886   | 2.776 |              |      |       |
|           | DBA5 | 0.878   | 2.622 |              |      |       |
| ATT       | ATT1 | 0.741   | 1.385 | 0.69         | 0.811 | 0.518 |
|           | ATT2 | 0.743   | 1.330 |              |      |       |
|           | ATT3 | 0.666   | 1.226 |              |      |       |
|           | ATT5 | 0.728   | 1.296 |              |      |       |
| PFR       | PFR2 | 0.904   | 3.247 | 0.902        | 0.932 | 0.773 |
|           | PFR3 | 0.805   | 1.941 |              |      |       |
|           | PFR4 | 0.915   | 3.326 |              |      |       |
|           | PFR5 | 0.889   | 2.695 |              |      |       |
| PPR       | PPR1 | 0.904   | 3.037 | 0.911        | 0.938 | 0.79  |
|           | PPR3 | 0.886   | 2.772 |              |      |       |
|           | PPR5 | 0.876   | 2.556 |              |      |       |
|           | PPR6 | 0.889   | 2.829 |              |      |       |
| PSR       | PSR1 | 0.88    | 2.564 | 0.904        | 0.933 | 0.778 |
|           | PSR3 | 0.901   | 3.090 |              |      |       |
|           | PSR4 | 0.911   | 3.235 |              |      |       |
|           | PSR5 | 0.833   | 2.141 |              |      |       |
| Trust     | Trust2 | 0.785   | 1.708 |              |      |       |
|           | Trust3 | 0.768   | 1.723 |              |      |       |
|           | Trust4 | 0.799   | 1.870 | 0.832        | 0.881 | 0.598 |
|           | Trust5 | 0.751   | 1.621 |              |      |       |
|           | Trust6 | 0.763   | 1.563 |              |      |       |
Table 6. Discriminant validity (Fornell–Larcker criterion).

|       | BI   | DBA  | ATT  | PFR  | PPR  | PSR  | Trust |
|-------|------|------|------|------|------|------|-------|
| BI    | 0.71 |      |      |      |      |      |       |
| DBA   | -0.188 | 0.88 |      |      |      |      |       |
| ATT   | 0.633 | -0.192 | 0.72 |      |      |      |       |
| PFR   | -0.163 | 0.844 | -0.189 | 0.879 |      |      |       |
| PPR   | -0.211 | 0.866 | -0.227 | 0.877 |      |      | 0.889 |
| PSR   | -0.229 | 0.824 | -0.222 | 0.835 | 0.872 | 0.882 |       |
| Trust | 0.511 | -0.409 | 0.537 | -0.405 | -0.447 | -0.443 | 0.773 |

4.2.2. Hypothesis Testing

The completed results of the hypothesis testing for the structural model are presented in Table 7, with eight of the ten hypotheses being confirmed by the survey data.

Path coefficients and hypothesis testing are shown in Figure 2; $\beta$ represents the path coefficient, which describes the relationships between the latent variables in the structural model. The $p$-value is used to disclose the significance level in hypothesis testing. In addition, we use coefficients of determination ($R^2$), effect sizes ($f^2$), and predictive relevance ($Q^2$) to provide additional insights about the quality of the PLS path model estimations.

For hypothesis H1, a significant positive correlation can be seen between attitude and behavioral intention ($\beta = 0.501; p < 0.001$). Therefore, H1 is confirmed. Trust has a significant positive effect on both ATT and BI, because the truth-related hypothesis H2a ($\beta = 0.550; p < 0.001$) and H2b ($\beta = 0.242; p < 0.001$) are shown to be significant. Similarly, among the six hypotheses associated with perceived risk, H3a ($\beta = -0.227; p < 0.05$), H3b ($\beta = 0.118; p < 0.05$), and H4 ($\beta = -0.262; p < 0.01$) are supported. However, H5a ($\beta = 0.014$) and H5b ($\beta = 0.033$) are not verified. H5c ($\beta = 0.128; p < 0.05$) is significant with a reverse effect on BI, which differs from the original hypothesis. In addition, H6 ($\beta = 0.866; p < 0.001$) is proven to have a significant positive effect.

Table 7. Path coefficients and hypothesis testing.

| Hypothesis | Path   | $f^2$ | T Statistics | $p$ Values | Path Coefficient | Bca (2.5; 97.5)% | Result       |
|------------|--------|------|--------------|------------|------------------|------------------|--------------|
| H1         | ATT → BI | 0.323 | 11.73 | 0.000 | 0.501 | (0.411; 0.578) | Supported |
| H2a        | Trust → ATT | 0.356 | 14.09 | 0.000 | 0.550 | (0.469; 0.621) | Supported |
| H2b        | Trust → BI | 0.063 | 5.071 | 0.000 | 0.242 | (0.145; 0.333) | Supported |
| H3a        | PSR → Trust | 0.015 | 2.585 | 0.010 | -0.227 | (-0.393; -0.050) | Supported |
| H3b        | PSR → BI | 0.007 | 2.060 | 0.039 | -0.118 | (-0.236; -0.012) | Supported |
| H4         | PPR → Trust | 0.014 | 2.608 | 0.009 | -0.262 | (-0.466; -0.073) | Supported |
| H5a        | PFR → Trust | 0.000 | 0.181 | 0.856 | 0.014 | (0.145; 0.163) | Not |
| H5b        | PFR → ATT | 0.001 | 1.002 | 0.316 | 0.033 | (-0.034; 0.097) | Not |
| H5c        | PFR → BI | 0.009 | 2.253 | 0.024 | 0.128 | (0.016; 0.242) | Not |
| H6         | DBA → PPR | 3.011 | 47.853 | 0.000 | 0.866 | (0.825; 0.896) | Supported |

Figure 2. Structural model (**p < 0.001, *p < 0.01, *p < 0.05).
According to criterion mentioned in [95], $R^2$ is used to evaluate predictive performance. If its value is above zero, the latent constructs are explained as exhibiting predictive relevance with the thresholds of 0.75, 0.50, and 0.25, which measure the strong, moderate, or weak predictive accuracy, respectively. The value of $f^2$ is used to measure the effect size of a given construct, with the thresholds of 0.02, 0.15, and 0.35 corresponding to weak, medium, and strong effect sizes, respectively. A blindfolding procedure was performed to assess the predictive relevance $Q^2 (>0)$. The results of $R^2$ and $Q^2$ are depicted in Table 8.

**Table 8. Values of $R^2$ and $Q^2$.**

|   | $R^2$ | Adjusted $R^2$ | $Q^2$ |
|---|-------|----------------|------|
| BI | 0.447 | 0.443          | 0.218|
| ATT | 0.289 | 0.286          | 0.146|
| PPR | 0.751 | 0.750          | 0.588|
| Trust | 0.212 | 0.207          | 0.123|

We used the adjusted $R^2$ value as the criterion. The results show that 28.6% of ATT variance was explained by trust, 75.0% of variance in PPR was explained by DBA, and 20.7% of variance in trust was explained by PSR and PPR. The 44.3% variance in BI was explained by antecedent variables in the model. In terms of variance interpretation, we can see that PPR has strong prediction accuracy. BI, ATT, and trust levels are relatively moderate. In addition, the path model has predictive relevance for endogenous structures, as all $Q^2$ values are above zero. The influence of ATT $\rightarrow$ BI and DBA $\rightarrow$ PPR are at a medium level, while trust has a great influence on ATT.

5. Discussion

The results of our analysis indicate that eight of the ten hypotheses we developed are supported. In this section, we further discuss and reveal the relationship among three types of perceived risk, trust, attitudes, and BI in order to answer RQ1 and RQ2.

In ICV, data services involving in audio and video, fingerprinting, and other profiles carry potential risks for users. For this reason, automakers, OEM, or SP need to gain trust from drivers and passengers through corresponding protection mechanisms. If users maintain trust in IVI data services from SP, their attitude is affected, while the BI becomes stronger. In this study, we assume that trust is influenced by the factors of perceived security, privacy, and performance risk when using IVI data services. In general, the less risk users perceive, the more trust is obtained, which has been verified by [96].

We find that PSR has a direct negative impact on trust and BI, which is consistent with the results of Anthony et al. [68] on electronic systems. Considering that ICV data services have certain potential security vulnerabilities, such as tracking and positioning, executing wrong instructions, and even endangering national security and public interests, this directly reduces willingness to use.

The results show that PPR can degrade trust among ICV users. Meanwhile, DBA has a significant positive impact on PPR, i.e., users’ DBA aggravates PPR. Similarly, the study of ICV services proves that users’ concern about disclosure of personal information increase PPR [42]. This anxiety reflects users’ worries and fears that automakers, SP, and even hackers may collect or steal individuals’ privacy data without authorization. In particular, network hacking has gradually developed as a common threat during the stage of data transmission, sharing, storage. When users are aware of uncertainty or the mechanism is not transparent among ICV data services, the perception of privacy concerns rises [51].

It is worth noting that 29.4% and 27.7% of respondents scored the items of PSR and PPR between 1–3, respectively, i.e., those respondents did not think that trust toward ICV data service was affected by potential PSR and PPR. On the one hand, this can be explained by the widespread popularity of smart devices and mobile applications, which has promoted users’ tolerance for data security and privacy matters such as the frequent use of face and voice recognition and fingerprint collection on smart phones. ICV can be
viewed as large mobile terminals [97], meaning that users may be more receptive towards data acquisition authorization and storage requests, such as providing phone numbers, call records, location, storage space, and even biological information in order to improve the quality of service. On the other hand, various countries have introduced relevant laws and policies in recent years to strengthen data security and privacy management, especially for IoV, ICV, and autonomous driving. ICV data collection, storage, and commercial usage should be managed and follow strict legal regulations in order to avoid data security and privacy loopholes. The implementation of these policies and regulations can help to improve users’ sense of security and reduce DBA.

Different from the previous hypothesis, PFR does not affect trust and attitude significantly. The reasons for this can be explained as follows. The perceived performance of IVI data services in ICVs includes function, usage permissions, protective measures, occupants’ data rights, etc., which are directly linked to BI rather than influenced through intermediary factors (e.g., trust, attitude). The drivers and passengers obtain the expected performance results only when they experience the relevant functions of the data service. The cost of PFR (e.g., weak data protection) is offset by the perceived benefits (e.g., normal use of data services). In a study of online banking, Lee [98] has found that perceived risks and benefits have opposite effects on attitudes, while Sythe et al. [80] have identified perceived benefits as positive predictors of users’ willingness to visit and make purchases from online stores. Therefore, when the two are in balance, the effect of PFR on trust and ATT is not obvious.

In summary, the above statement reveals the relationship between perceived risk and trust, meaning that RQ1 can be answered.

However, it can be seen that PFR has a positive impact on BI, which is contrary to the study of perceived autonomous vehicle performance risk in [99]. The reason for this can be explained by variations in users’ perceptual abilities and psychological willingness. The characteristics (e.g., age, gender, and past experience) among different users group affect individuals’ privacy management strategies. Wolf has found that girls are more disciplined than boys in terms of personal and interpersonal privacy management and that people who experience privacy turmoil adopt more personal stringent privacy management strategies [100]. Communication Privacy Management theory suggests that the privacy management process becomes more complex as individuals age [101]. In addition, the big five personality model suggests that extraversion, agreeableness, conscientiousness, neuroticism, openness, and other personality traits may affect users’ attention to information privacy [103]. A higher PFR represents users’ high attention to performance loss. Among the four items of PFR, PFR3 (Mean = 4.924, SD = 1.73, Median = 5) has the highest average score, meaning that the respondents are most worried about inability to use the functions of relevant IVI data services when declining permissions around collection and authorization. PFR2 (Mean = 4.688, SD = 1.72, Median = 5) and PFR4 (Mean = 4.774, SD = 1.65, Median = 5) are both lower than the overall average score (Mean = 4.797), meaning that protection measures around data and privacy are of less concern and can achieve user expectations to an extent.

In term of BI, we can see that the average score of BI3 (Mean = 5.876, SD = 0.87, Median = 6) and BI6 (Mean = 5.932, SD = 0.82, Median = 6) is significantly higher compared with BI1 (Mean = 5.408, SD = 0.98, Median = 5) and BI5 (Mean = 5.562, SD = 1.01, Median = 6). This means that the participants’ willingness to use data services is higher. In other words, users have more concerns about the function of IVI data services that cannot be achieved or meet expectations. In this way, their BI may be increased due to the convenience of IVI data services. In addition, national and local governments pay more attention to data security and individual privacy via comprehensive and strict legal regulations. Although users have potential concerns about the expected performance of data services, it is highly likely that they will continue to increase the use of relevant data services based on their trust in the government.

In terms of attitude towards ICV data services, respondents scored higher on average in the four items (Mean = 5.762, SD = 0.89, Median = 6), and generally show a positive
attitude. Among them, 93.15% of respondents report a positive attitude score between 5 and 7, with 5.9% of respondents remaining neutral and only 0.95% having a relatively negative attitude towards ICV data services. This result greatly increases the BI of occupants concerning the use of ICV data services. Trust is an important factor that can affect attitude and BI, as verified by relevant studies [104,105]. The more users trust ICV data services, the more positive their attitude towards such services becomes, making them more inclined to use ICV data services. Considering that attitude is an important factor influencing users’ BI (total effect = 0.501), the more positive users are towards ICV data service, the stronger their BI to use becomes. Similar findings have been found in studies of acceptance of autonomous driving vehicles [106] and ICV IVI [107]. Therefore, RQ2 is answered.

5.1. Implications

Based on the results of our empirical analysis, the theoretical and practical significance of this research can be summarized as follows.

In terms of theoretical implications, this paper retains the critical path from attitude to BI on the basis of TPB model and highlights the relationship between perceived risk and trust in ICV data services with aim of providing a unique perspective for future data privacy and security research. First of all, there is little research on risk and trust in the context of ICV data services. Our research results show that perceived risk and trust have an important impact on the attitude and behavior of users of ICV data services. Second, risk analysis is vital in research on emerging technologies. According to the hierarchical structure of perceived risks, we subdivide risk into perceived security risk, perceived privacy risk, and perceived performance risk. Compared with the general study of ICV potential risks, the focus can be shifted to more detailed risk levels. Finally, data breach anxiety is introduced as the factor for PPR of ICV data service. If a data breach occurs via IoV, serious consequences can result for both occupants and organizations.

In terms of practical significance, our research results show that risk perception affects users’ trust, ATT, and BI towards ICV data services to varying degrees, with perceived risk and trust as important factors for users considering the adoption of ICV data services. Although ICV is one of the development directions of future vehicles, many drivers and passengers have concerns and doubts about the data services of ICV. Risk perception is closely related to trust, with lower risk perception making it the more beneficial to establish and consolidate user trust. Therefore, automakers, OEM, and SP need to strengthen guidance in order to help users to establish correct risk perceptions. Meanwhile, measures should be taken to solve potential risk problems and increase user trust. Specifically, in terms of data security, it is necessary to strengthen protection measures in order to prevent data from being monitored, damaged, tampered with, and abused. In terms of privacy, users’ data rights should receive sufficient attention and information collection mechanisms should be more transparent and standardized. In terms of service performance, user experience needs to be improved in terms of functions and permissions. In addition, this research can help government agencies to learn about users’ attitude towards ICV data services and revise any related regulations and policies accordingly in the era of IoV.

5.2. Limitations

In this section, we present limitations of the present research. First, most participants in our study were from eastern, northern, and central China, especially Shandong, Beijing, Zhejiang, Guangzhou, and other provinces, while the coverage rate in Western China was low. Second, the questionnaires were collected mainly through online survey platforms or social media in order to maintain social distancing during the COVID-19 pandemic. Only people with internet access were able to fill out questionnaires, making it impossible to observe the real behaviors of interviewees during the process of filling out the questionnaire. In future research, both online and offline collection should be combined to obtain more representative questionnaire responses. Third, due to the functional differences among ICV, users may not experience all kind of data service. The level of risk perception and trust may change in the future as users increase their knowledge of ICV and gain a deeper
understanding of IVI systems. Therefore, it is necessary to observe the attitudes and BI of ICV users over a long period of time in order to determine how trust evolves as users are exposed to more interactions with ICV.

6. Conclusions
In this paper, we have proposed a theoretical model to reveal the effect of perceived risks toward users’ trust, attitude, and behavioral intention (BI) when using the in-vehicle infotainment (IVI) data services of intelligent connected vehicles. In the model, the perceived risks are divided into perceived security risk (PSR), perceived privacy risk (PPR), and perceived performance risk (PFR). Specifically, PSR reduces users’ trust and BI, PPR has a negative effect on trust, and DBA aggravates PPR. Our results show that the respondents scored higher on average for attitude and BI when they perceived fewer data and privacy concerns in IVI data services. The BI has been affected by the factors of PSR, PFR, trust, and attitude, which are able to explain 44.3% of variance.

With their growing commercialization, the market penetration of ICV can be expected to increased, and more and more drivers and passengers will become ICV users in the future. As such, we suggest exploration of the role of other factors, such as privacy norms and past experiences, in order to further clarify changes with increased usage of ICV data services. The impact of personality characteristics on use of IVI data services may relate to the results considering the differences among occupants. In addition, the specific research in Chinese ICV test and demonstration zones is an interesting direction to focus on, as this could reveal the attitudes of local people attitudes and their perception of the risks involved in IVI data services.

Author Contributions: Conceptualization, Z.Y.; methodology, Z.Y.; validation, Z.Y. and K.C.; formal analysis, Z.Y. and K.C.; investigation, Z.Y. and K.C.; writing—original draft preparation, Z.Y. and K.C.; writing—review and editing, Z.Y. and K.C.; visualization, K.C. and Z.Y.; supervision, Z.Y.; funding acquisition, Z.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research is part of the Social Science Planning Research Project of Shandong Province with Grant Number 21DXWJ06. The Article Processing Charge was provided by Future Plan for Young Scholars of Shandong University.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The public survey data related to this paper have been presented, and the other data are securely protected by the researchers.

Acknowledgments: The authors would like to express their gratitude to the anonymous reviewers for the valuable comments.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

| Abbreviation | Definition                          |
|--------------|------------------------------------|
| ATT          | Attitude                           |
| BI           | Behavioral Intention               |
| DBA          | Data Breach Anxiety                |
| ICV          | Intelligent Connected Vehicle      |
| IoV          | Internet of Vehicles               |
| ITS          | Intelligent Transportation System   |
| IVI          | In-Vehicle Infotainment            |
| OEM          | Original Equipment Manufacture      |
| PSR          | Perceived Security Risk            |
| PPR          | Perceived Privacy Risk             |
| PFR          | Perceived Performance Risk         |
| PLS          | Partial Least Squares              |
Appendix A. Typical ICV Models

Table A1. Typical ICV models.

| Models           | Release Time | Vehicular Sensor                     |
|------------------|--------------|--------------------------------------|
| Tesla Model Y    | 2019         | 8 cameras                            |
|                  |              | 1 Millimeter wave radar              |
|                  |              | 12 Ultrasonic sensors                |
| Ford EVOS        | 2021         | 6 cameras                            |
|                  |              | 5 Millimeter wave radar              |
|                  |              | 12 Ultrasonic radars                 |
| BMW iX           | 2021         | 5 cameras                            |
|                  |              | 5 Radar sensors                      |
|                  |              | 12 Ultrasonic sensors                |
| XPENG P5         | 2021         | 13 cameras                           |
|                  |              | 2 Lidar                              |
|                  |              | 5 Millimeter wave radars             |
|                  |              | 12 Ultrasonic sensors                |
| ROEVE RX5        | 2022         | 11 cameras                           |
|                  |              | 3 Millimeter wave radar              |
|                  |              | 12 Ultrasonic sensors                |
|                  |              | 1 Steering wheel capacitance sensor  |

Appendix B. Questionnaire Item

Table A2. Construct items.

| Construct | Item and Content                                                                                      | Source          |
|-----------|-------------------------------------------------------------------------------------------------------|-----------------|
| PSR       | PSR1: I concern the overall security of privacy and data collected by ICV (e.g., driving track, location, habit and inter/intra-environment etc.). PSR2: I concern hackers intercept or crack transmitted data via IoV and then execute wrong instructions, which lead to accidents. § PSR3: When data transfer (e.g., vehicle-to-home), I concern automaker, OEM or SP will disregard the data security issue. PSR4: I concern automaker, OEM or SP don’t provide data protection and security measures (e.g., unauthorized access). PSR5: I concern the occupants are not promptly alerted to the risks when trigger data protection procedure. PSR6: I concern the collected and stored data from occupants has the risk of be monitored, damaged, tampered, abused. § PSR7: I concern the data (e.g., landform) collected by ICV may pose risks to national security, public interests of organizations or individuals. § | Zhang et al. [55] Yenisey et al. [48] Lee [98] |
| PPR       | PPR1: I concern automaker, OEM or SP use the collected data for other purposes without authorization. PPR2: I concern personal sensitive or private data can’t be deleted timely when stop to use or change ICV. § PPR3: I concern ICV automatically collect facial, vocal print, gait and other biometric/behavioral features of occupants and surrounding people without authorization. PPR4: I concern the collected privacy info, IVI usage and tracking recorder are shared by automaker, OEM or SP without authorization. § PPR5: I concern automaker, OEM or SP collect occupants’ movement and location records. † PPR6: I concern automaker, OEM or SP do not anonymize or encrypt the collected data of occupants when using IVI data services. † | Featherman et al. [36] Zhang et al. [55] Kim et al. [67] |
### Table A2. Cont.

| Construct | Item and Content | Source |
|-----------|-----------------|--------|
| **PFR** | PFR1: I concern IVI data services cannot perform well and affect the personalized IVI demands of occupants. § | Featherman et al. [36] |
| | PFR2: I concern the data security module of ICV is not strong enough. | Littler et al. [79] |
| | PFR3: I concern functions and permissions in IVI data service unable to use When declining collection, authorization requests or privacy clauses on ICV. | Zhao et al. [108] |
| | PFR4: I concern the privacy protections offered by ICV will fall short of expectations. | |
| | PFR5: I concern the privacy data collected by ICV cannot be normally consulted, copied, migrated and deleted, thus affecting the data rights of occupants. † | |
| **DBA** | DBA1: I concern hackers steal the account and password of IVI system. | Keszey [109] |
| | DBA2: During driving, I concern the real-time location, trajectory and other data will be leaked, which is easy to track and locate occupants. § | Elhai et al. [51] |
| | DBA3: I concern hackers obtain the cloud data transmitted from ICV to automaker and SP. | |
| | DBA4: I concern sensitive pictures, videos, audio (e.g., chat) collected by sensors inside and outside the car are leaked. | |
| | DBA5: I concern unauthorized access to personal data from connected devices. | |
| **Trust** | Trust1: I think the provided IVI data service are true. § | Pillai & Sivathanu [110] |
| | Trust2: I think the protection mechanism of automaker and SP for collected data is reliable with the constraints of laws. | |
| | Trust3: I think automaker and SP are capable to ensure the collected privacy and data security from occupants when using ICV. | |
| | Trust4: I think the data security mechanisms established by automaker, OEM and SP are effective. † | |
| | Trust5: I think IoV SP have established emergency mechanisms to take timely measures in case of data security incidents. † | |
| | Trust6: I think personal privacy data collected by ICV will be transmitted and stored in accordance with the law and strict supervision. † | |
| **ATT** | ATT1: I think it is a good choice to use IVI data services on ICV. | Taylor & Todd [111] |
| | ATT2: I think it is a wise choice to use IVI data services of ICV when guaranteeing the data and privacy security. | |
| | ATT3: I prefer to use the convenient and efficient IVI data service when perceived privacy and security risks are controllable. | |
| | ATT4: I think IVI data services are satisfactory and can improve comfort level of driving when PSR and PPR are manageable. § | Wu et al. [43] |
| | ATT5: I hold relatively positive attitude towards data collection for IVI, driving assistance and other functions supported by ICV. | |
| | ATT6: I think ICV data collection can provide important support for personalized driving experience. § | |
| **BI** | BI1: Under the data security regulations, I will authorize automaker, OEM or SP to obtain driving data for better personalized IVI. | Kim et al. [40] |
| | BI2: For the next purchase, I’ll opt for ICV with features of IoV and IVI. § | |
| | BI3: I will gradually increase the usage frequency of IVI data service on ICV to get better driving experience. | |
| | BI4: With same price, I prefer to buy ICV with powerful functions of data security and privacy. § | Yu et al. [107] |
| | BI5: Under the data security regulations, I will allow automakers, OEM or SP to collect data for better IVI services. | Walter et al. [42] |
| | BI6: I will use IVI data service when data security and privacy are guaranteed. | |

†: self-developed Items; §: Items were removed after evaluation.

**References**

1. Liu, J.; Liu, J. Intelligent and connected vehicles: Current situation, future directions, and challenges. *IEEE Commun. Stand. Mag.* 2018, 2, 59–65. [CrossRef]
2. Statista, Size of the Global Connected Car Fleet in 2021, with a Forecast for 2025, 2030, and 2035, by Region. 2021. Available online: https://www.statista.com/statistics/1155517/global-connected-car-fleet-by-market/#statisticContainer (accessed on 10 June 2022).
3. European Data Protection Board, Guidelines 01/2020 on Processing Personal Data in the Context of Connected Vehicles and Mobility Related Applications. 2021. Available online: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012020-processing-personal-data-context_en (accessed on 10 June 2022).
4. Official Journal of the European Union, General Data Protection Regulation. 2016. Available online: https://gdpr-info.eu/ (accessed on 10 June 2022).
35. Bhatnagar, A.; Misra, S.; Rao, H.R. On risk, convenience, and internet shopping behavior. Commun. ACM 2000, 43, 98–105. [CrossRef]
36. Featherman, M.S.; Pavlou, P.A. Predicting e-services adoption: a perceived risk facets perspective. Int. J. Hum.-Comput. Stud. 2003, 59, 451–474. [CrossRef]
37. Mittgen, C.L.; Popović, A.; Oliveira, T. Determinants of end-user acceptance of biometrics: Integrating the “big 3” of technology acceptance with privacy context. Decis. Support Syst. 2013, 56, 103–114. [CrossRef]
38. Vandezande, N.; Janssen, K. The its directive: more than a timeframe with privacy concerns and a means for access to public data for digital road maps? Comput. Law Secur. Rev. 2012, 28, 416–428. [CrossRef]
39. Marell, A.; Westin, K. Intelligent transportation system and traffic safety—Drivers perception and acceptance of electronic speed checkers. Transp. Res. Part C 1999, 7, 131–147. [CrossRef]
40. Kim, J.; Kim, S.; Nam, C. User resistance to acceptance of in-vehicle infotainment (ivi) systems. Telecommun. Policy 2016, 40, 919–930. [CrossRef]
41. Maeng, K.; Kim, W.; Cho, Y. Consumers’ attitudes toward information security threats against connected and autonomous vehicles. Telemat. Inform. 2021, 63, 101646. [CrossRef]
42. Walter, J.; Abendroth, B. On the role of informational privacy in connected vehicles: A privacy-aware acceptance modelling approach for connected vehicular services. Telemat. Inform. 2020, 49, 101361. [CrossRef]
43. Wu, Z.; Zhou, H.; Xi, H.; Wu, N. Analysing public acceptance of autonomous buses based on an extended tam model. IET Intell. Transp. Syst. 2021, 15, 1318–1330. [CrossRef]
44. Lee, J.; Lee, D.; Park, Y.; Lee, S.; Ha, T. Autonomous vehicles can be shared, but a feeling of ownership is important: Examination of the influential factors for intention to use autonomous vehicles. Transp. Res. Part C 2019, 107, 411–422. [CrossRef]
45. Kapser, S.; Abdelrahman, M. Acceptance of autonomous delivery vehicles for last-mile delivery in germany—Extending utaut2 with risk perceptions. Transp. Res. Part C 2020, 111, 210–225. [CrossRef]
46. Laghari, A.A.; Wu, K.; Laghari, R.A.; Ali, M.; Khan, A.A. A Review and State of Art of Internet of Things (IoT). Arch. Comput. Methods Eng. 2022, 29, 1395–1413. [CrossRef]
47. Kaur, K.; Rampersad, G. Trust in driverless cars: Investigating key factors influencing the adoption of driverless cars. J. Eng. Technol. Manag. 2018. [CrossRef]
48. Yunisey, M.M.; Ozok, A.A.; Salvendy, G. Perceived security determinants in e-commerce among turkish university students. Behav. Inf. Technol. 2005, 24, 259–274. [CrossRef]
49. Jarvenpaa, S.L.; Todd, P.A. Consumer reactions to electronic shopping on the World Wide Web. Int. J. Electron. Commer. 1996, 1, 59–88. [CrossRef]
50. Grewal, D.; Goltlieb, J.; Marmorstein, H. The moderating effects of message framing and source credibility on the price-perceived risk relationship. J. Consum. Res. 1994, 21, 145–153. [CrossRef]
51. Elhai, J.D.; Hall, B.J. Anxiety about internet hacking: Results from a community sample. Comput. Hum. Behav. 2016, 54, 180–185. [CrossRef]
52. Gefen, D.; Karahanna, E.; Straub, D.W. Trust and TAM in online shopping: An integrated model. MIS Q. 2003, 27, 51–90. [CrossRef]
53. Wu, B.; Zhang, C. Empirical study on continuance intentions towards E-Learning 2.0 systems. Behav. Inf. Technol. 2014, 33, 1027–1038. [CrossRef]
54. Liljamo, T.; Liimatainen, H.; Pöllänen, M. Attitudes and concerns on automated vehicles. Transp. Res. Part F 2018, 59, 24–44. [CrossRef]
55. Zhang, T.; Tao, D.; Qu, X.; Zhang, X.; Lin, R.; Zhang, W. The roles of initial trust and perceived risk in public’s acceptance of automated vehicles. Transp. Res. Part C 2019, 98, 207–220. [CrossRef]
56. Vijayasarathy, L.R. Predicting consumer intentions to use on-line shopping: The case for an augmented technology acceptance model. Inf. Manag. 2004, 41, 747–762. [CrossRef]
57. Hoffman, D.L.; Novak, T.P.; Peralta, M. Building consumer trust online. Commun. ACM 1999, 42, 80–85. [CrossRef]
58. Yang, H.; Lee, H.; Zo, H. User acceptance of smart home services: An extension of the theory of planned behavior. Ind. Manag. Data Syst. 2017, 117, 68–89. [CrossRef]
59. Jarvenpaa, S.L.; Tractinsky, N.; Saarinen, L. Consumer trust in an Internet store: A cross-cultural validation. J. Comput.-Mediat. Commun. 1999, 5, 59–88. [CrossRef]
60. Fang, J.; Shao, P.; Lan, G. Effects of innovativeness and trust on web survey participation. Comput. Hum. Behav. 2009, 25, 144–152. [CrossRef]
61. Muangmee, C.; Kot, S.; Meekaewkunchorn, N.; Kassakorn, N.; Khalid, B. Factors Determining the Behavioral Intention of Using Food Delivery Apps during COVID-19 Pandemics. J. Theor. Appl. Electron. Commer. Res. 2021, 16, 1297–1310. [CrossRef]
62. Pavlou, P.A. Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model. Int. J. Electron. Commer. 2003, 7, 101–134. [CrossRef]
63. Bansal, P.; Kockelman, K.M.; Singh, A. Assessing public opinions of and interest in new vehicle technologies: An austin perspective. Transp. Res. Part C 2016, 67, 1–14. [CrossRef]
64. Kolsaker, A.; Payne, C. Engendering trust in e-commerce: A study of gender-based concerns. Mark. Intell. Plan. 2002, 20, 206–214. [CrossRef]
65. König, M.; Neumayr, L. Users’ resistance towards radical innovations: The case of the self-driving car. *Transp. Res. Part F* 2017, 44, 42–52. [CrossRef]

66. Ponte, E.B.; Carvaljal-Trujillo, E.; Escobar-Rodriguez, T. Influence of trust and perceived value on the intention to purchase travel online: integrating the effects of assurance on trust antecedents. *Tour. Manag.* 2015, 47, 286–302. [CrossRef]

67. Kim, D.J.; Ferrin, D.L.; Rao, H.R. A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decis. Support Syst.* 2008, 44, 544–564. [CrossRef]

68. Miyazaki, A.D.; Fernandez, A. Consumer perceptions of privacy and security risks for online shopping. *J. Consum. Aff.* 2001, 35, 27–44. [CrossRef]

69. Kyriakidis, M.; Happee, R.; Winter, J.D. Public opinion on automated driving: Results of an international questionnaire among 5000 respondents. *Transp. Res. Part F* 2015, 32, 127–140. [CrossRef]

70. Glancy, D.J. Privacy in autonomous vehicles. *Santa Clara Law Rev.* 2012, 52, 1171–1239.

71. Martin, D.K.; Borah, A.; Palmatier, R.W. Data Privacy: Effects on Customer and Firm Performance. *J. Mark.* 2016. [CrossRef]

72. Bhattacharjee, A. Individual Trust in Online Firms: Scale Development and Initial Test. *J. Manag. Inf. Syst.* 2002, 19, 211–241. [CrossRef]

73. Metzger, M.J. Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *J. Comput.-Mediat. Commun.* 2004, 9, JCMC942. [CrossRef]

74. Kaplan, L.B.; Szybillo, G.J.; Jacoby, J. Components of perceived risk in product purchase: A cross-validation. *J. Appl. Psychol.* 1974, 59, 287–291. [CrossRef]

75. Cunningham, L.E.; Gerlach, J.H.; Harper, M.D.; Young, C.E. Perceived risk and the consumer buying process: Internet airline reservations. *Int. J. Serv. Ind. Manag.* 2005, 16, 357–372. [CrossRef]

76. Cunningham, S.M. The major dimensions of perceived risk. In *Risk Taking and Information Handling in Consumer Behavior*; Cox, D.F., Ed.; Harvard University Press: Cambridge, MA, USA, 1967.

77. Bhattacharjee, A. Individual Trust in Online Firms: The Relative and Temporal Effects of Antecedent Beliefs. *Int. J. E-Bus. Res.* 2006, 2, 21–38. [CrossRef]

78. George, O.J.; Ogunkoya, O.A.; Lasisi, J.O.; Elumah, L.O. Risk and Trust in Online Shopping: Experience from Nigeria. *Int. J. Afr. Asian Stud.* 2015, 11, 71–77.

79. Littler, D.; Melanthiou, D. Consumer perceptions of risk and uncertainty and the implications for behaviour towards innovative retail services: The case of internet banking. *J. Retail. Consum. Serv.* 2006, 13, 431–443. [CrossRef]

80. Forsythe, S.; Liu, C.; Shannon, D.; Liu, C.G. Development of a scale to measure the perceived benefits and risks of online shopping. *J. Interact. Mark.* 2006, 20, 55–75. [CrossRef]

81. Park, J.; Lennon, S.J.; StoeI, L. On-line product presentation: Effects on mood, perceived risk, and purchase intention. *Psychol. Mark.* 2005, 22, 695–719. [CrossRef]

82. Lee, H.H.; Kim, J.; Fiore, A.M. Affective and Cognitive Online Shopping Experience: Effects of Image Interactivity Technology and Experimenting with Appearance. *Comm. Text. Res.* 2010, 28, 140–154. [CrossRef]

83. Igbaria, M.; Parasuraman, S. A path analytic study of individual characteristics, computer anxiety and attitudes toward microcomputers. *J. Manag.* 1989, 15, 373–388. [CrossRef]

84. Meuter, M.L.; Bitner, M.J.; Ostrom, A.L.; Brown, S.W. Choosing among alternative service delivery modes: An investigation of customer trial of self-service technologies. *J. Mark.* 2005, 69, 61–83. [CrossRef]

85. Dinev, T.; Hart, P. Internet privacy concerns and their antecedents—Measurement validity and a regression model. *Behav. Inf. Technol.* 2004, 23, 413–422. [CrossRef]

86. Solove, D.J.; Citron, D.K. Risk and anxiety: A theory of data breach harms. *SSRN Electron.* 2016, 96, 737–786. [CrossRef]

87. Chakraborty, R.; Lee, J.; Bagchi-Sen, S.; Upadhyaya, S.; Rao, H.R. Online shopping intention in the context of data breach in online retail stores: An examination of older and younger adults. *Decis. Support Syst.* 2016, 83, 47–56. [CrossRef]

88. Cheyun, The ICV Sales Beyond 2.7 Million in 2021. 2022. Available online: http://ww.cheyun.com/articleDetail/45431 (accessed on 15 May 2022).

89. Ketchen, D.J., Jr. A primer on partial least squares structural equation modeling. *Long Range Plan.* 2013, 46, 184–185. [CrossRef]

90. Chin, W.W.; Marcolin, B.L.; Newsted, P.R. A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study. *Inf. Syst. Res.* 2003, 14, 189–217. [CrossRef]

91. Lee, L.; Petter, S.; Fayard, D.; Robinson, S. On the use of partial least squares path modeling in accounting research. *Int. J. Account. Inf. Syst.* 2011, 12, 305–328. [CrossRef]

92. do Valle, P.O.; Assaker, G. Using Partial Least Squares Structural Equation Modeling in Tourism Research: A Review of Past Research and Recommendations for Future Applications. *J. Travel Res.* 2015, 55, 1–14. [CrossRef]

93. Hair, J., Jr.; Sarstedt, M.; Hopkins, L.; Ringle, C.M. When to use and how to report the results of PLS-SEM. *Eur. Bus. Rev.* 2019, 31, 2–24. [CrossRef]

94. Hair, J.F.; Hult, G.T.M.; Ringle, C.; Sarstedt, M. A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM), 2nd ed.; SAGE Publications, Inc.: Thousand Oaks, CA, USA, 2017.
96. Ajenaghughrure, I.B.; Sousa, S.; Lamas, D. Risk and Trust in artificial intelligence technologies: A case study of Autonomous Vehicles. In Proceedings of the 2020 13th International Conference on Human System Interaction (HSI), Tokyo, Japan, 6–8 June 2020; pp. 118–123. [CrossRef]

97. Yu, Z.; Jin, D.; Zhai, C.; Ni, W.; Wang, D. Internet of vehicles empowered mobile media: Research on mobile-generated content (mogc) for intelligent connected vehicles. *Sustainability* 2021, 13, 3538. [CrossRef]

98. Lee, M.C. Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit. *Electron. Commer. Res. Appl.* 2009, 8, 130–141. [CrossRef]

99. Waung, M.; Mcauslan, P.; Lakshmanan, S. Trust and intention to use autonomous vehicles: Manufacturer focus and passenger control. *Transp. Res. Part F* 2021, 80, 328–340. [CrossRef]

100. Wolf, R.D. Contextualizing how teens manage personal and interpersonal privacy on social media. *New Media Soc.* 2020, 22, 1058–1075. [CrossRef]

101. Petronio, S.; Altman, I. *Boundaries of Privacy: Dialectics of Disclosure*; State University of New York Press: Albany, NY, USA, 2002. [CrossRef]

102. Tang, J.; Zhang, B.; Xiao, S. Examining the Intention of Authorization via Apps: Personality Traits and Expanded Privacy Calculus Perspectives. *Behav. Sci.* 2022, 12, 218. https://doi.org/10.3390/bs12070218.

103. Osatuyi, B. Personality traits and information privacy concern on social media platforms. *J. Comput. Inf. Syst.* 2015, 55, 11–19. [CrossRef]

104. Xu, Z.; Zhang, K.; Min, H.; Zhen, W.; Zhao, X.; Liu, P. What drives people to accept automated vehicles? findings from a field experiment. *Transp. Res. Part C* 2018, 95, 320–334. [CrossRef]

105. Dai, J.; Li, R.; Liu, Z. Does initial experience affect consumers’ intention to use autonomous vehicles? evidence from a field experiment in beijing. *Accid. Anal. Prev.* 2021, 149, 105778. [CrossRef]

106. Erskine, M.A.; Brooks, S.; Greer, T.H.; Apigian, C. From driver assistance to fully-autonomous: Examining consumer acceptance of autonomous vehicle technologies. *J. Consum. Mark.* 2020, 37, 883–894. [CrossRef]

107. Yu, Z.; Jin, D. Determinants of Users’ Attitude and Intention to Intelligent Connected Vehicle Infotainment in the 5G-V2X Mobile Ecosystem. *Int. J. Environ. Res. Public Health* 2021, 18, 10069. [CrossRef]

108. Zhao, A.L.; Hanmer-Lloyd, S.; Ward, P.; Goode, M. Perceived risk and chinese consumers’ internet banking services adoption. *Int. J. Bank Mark.* 2008, 26, 505–525. [CrossRef]

109. Keszey, T. Behavioural intention to use autonomous vehicles: Systematic review and empirical extension. *Transp. Res. Part C* 2020, 119, 102732. [CrossRef]

110. Pillai, R.; Sivathanu, B. Adoption of ai-based chatbots for hospitality and tourism. *Int. J. Contemp. Hosp. Manag.* 2020, 32, 3199–3226. [CrossRef]

111. Taylor, S.; Todd, P.A. Understanding information technology usage: A test of competing models. *Inf. Syst. Res.* 1995, 6, 144–176. [CrossRef]