Hindawi
Journal of Advanced Transportation
Volume 2022, Article ID 7588929, 11 pages
https://doi.org/10.1155/2022/7588929

Research Article

Sustainable Development of Shared Mobility in China in Relation to the Privacy Paradox of Users

Yuqin Li and Hanying Guo

School of Automobile and Transportation, Xihua University, Chengdu 610039, China

Correspondence should be addressed to Hanying Guo; 0120070011@mail.xhu.edu.cn

Received 14 August 2021; Revised 30 November 2021; Accepted 25 February 2022; Published 23 April 2022

Academic Editor: Jose E. Naranjo

Shared mobility is an important part of a smart city transportation system. However, during the short period it has been in effect, privacy leakages have frequently occurred, and as travellers are increasingly paying attention to their privacy, leakages hinder the rapid development of shared mobility. Therefore, it is important to explore the origin of the privacy paradox in the context of shared mobility and propose some targeted measures for improvement. The privacy paradox has been attested in numerous studies, where, despite their obvious concern that their privacy will be compromised, users continued to adopt services that may compromise it. This study constructs a model for the privacy paradox based on the theory of planned behaviour, privacy calculus theory, and construal level theory. A questionnaire survey was conducted with 301 Chinese college students to quantitatively analyse the relationship between the main factors of users' privacy paradox in the context of shared mobility. The study results showed that (a) the privacy paradox does exist in shared mobility among college students; (b) both perceived benefit and trust have a significant positive effect on near future disclosure intention, with trust being the prime motivator; (c) both privacy concern and perceived risk have significant negative effects on distant future disclosure intention, with privacy concern being the key ingredient; and (d) both near and distant future disclosure intentions have positive effects on privacy disclosure behaviour, with near future disclosure intention having a more significant influence. Further, to promote the healthy and sustainable development of China's shared mobility industry, countermeasures and suggestions have been proposed for users, ride-sharing enterprises, and the government according to the research results.

1. Introduction

Shared travel, an increasingly popular mode of travel that is based on mobile Internet, is an important component of the transportation system in smart cities. Its emergence has brought speed and convenience to daily life. The concept of shared mobility refers to the shared use of a form of transportation, such as bicycles, cars, scooters, or other transportation modes [1]. In China, the most popular modes of shared travel are cars, bikes, electric cars, and Internet buses, represented by companies such as DiDi Chuxing, Hello-Bike, Meituan, and Dudu Bus, respectively. In the previous decade, China witnessed a rapid increase in shared mobility. As per the data from the State Information Center, the scale of China's shared mobility market displayed an overall positive trend in growth from 2017 to 2019 [2]. Additionally, according to the data of Statistical Survey Report on Internet Development, Chinese online car hailing had a fluctuating growth trend. By the end of 2020, the number of registered users had reached 365 million [3]. Unfortunately, while users enjoy the efficiency and convenience engendered by shared mobility, they have also been confronted with the risk of privacy leakage. On the night of 9 July 2021, China's Cyberspace Administration reported about the illegal collection and use of personal information by DiDi. Consequently, 25 of its mobile applications were removed from application stores [4]. Moreover, on 26 January 2021, the Ministry of Industry and Information Technology revealed other illegal applications that infringed on the rights of users, such as Dongfeng Travel and Dingdang Travel [5].

Privacy is a comprehensive concept that spans across multidisciplinary fields, such as law, psychology, and sociology. It is broadly regarded as the subjective right of a person to protect personal interests, such as dignity, autonomy, or freedom [6]. With the continuous development of Internet technologies, the issue of network privacy has appeared at a historic moment. Jiang et al. [7] defined Internet privacy as personal information that consumers can protect and control. The advent of the Internet will enable high levels of connection between passengers and vehicles. Additionally, such a connection can result in a large amount of user data being generated, where the travel habits of pedestrians can be easily extracted [7]. This scenario leads to increased concerns regarding personal data privacy among users.

Alternatively, although people are concerned about the security of their personal information, they continue to engage in privacy disclosure. Scholars have called this inconsistency between the privacy concerns and disclosure behaviour of users the *privacy paradox* [8]. Numerous studies have demonstrated that trust [9], perceived benefit [10], and other factors can promote the active disclosure of users. Additionally, perceived risk [11] and privacy concerns [10] inhibit privacy disclosure. Based on these aforementioned aspects, this study considers privacy concern, perceived benefit, perceived risk, and trust as the influencing factors of the privacy paradox of shared travellers.

Chen et al. [12] proposed that college students experience great freedom on campus and that they can be considered a separate social group that exhibits complex and unique travel behaviours. This group is among the most important market segments of shared mobility owing to its low rate of car ownership, frequent mobility, high smartphone usage, tendency to share, and residence in urban commuting centres [13]. Therefore, college students can be used as an experimental group to help guide a wide range of future studies. Moreover, an in-depth study on the privacy paradox of college students may help to better understand the impact of the privacy paradox on other user groups of shared mobility [14].

This study focuses on the privacy paradoxes of shared mobility solutions—such as shared bikes, motorcycles, and cars—from various perspectives, such as from peer-to-peer sharing to travel. To explore the privacy paradox in the context of shared mobility, this study recruited 301 Chinese college students to fill in a questionnaire survey using a five-point Likert scale. Additionally, the theory of planned behaviour (TPB), privacy calculus theory (PCT), and construal level theory (CLT) were integrated to create a relatively comprehensive model in order to examine the privacy paradox among shared travellers and identify the mechanisms of their privacy disclosure behaviours. The research results of this study will help individual users, shared mobility enterprises, and the government to understand the privacy paradox in the context of shared mobility; moreover, it will have important guiding significance for promoting healthy and sustainable development in the shared mobility industry.

2. Literature Review and Theory

2.1. Theory of Planned Behaviour. TPB is the mainstream model for investigating individual behavioural choice; it has been proven to significantly improve the explanatory and predictive powers of behavioural research [15]. TPB was first proposed by Ajzen [16], whose research found that personal attitudes, personal subjective norms, and personal perceived behavioural control indirectly influence the final behaviour of an individual by influencing their will. Since then, numerous studies have modified the scope of the original attitudes and behaviours claimed by the theory. Conner et al. [17] added user intention, behavioural perceptions, and behavioural stability based on the original theory, thus enhancing the explanatory power of the model. Presently, TPB is used in many practical domains, such as online shopping [18], medical waste separation [19], driving [20], sports [21], eating [22], privacy paradox [23], and other practical areas related to behaviour.

According to TPB, the willingness to disclose information influences the privacy disclosure behaviour of users in the privacy paradox of shared mobility. Based on this rationale, this study considers the intention of privacy disclosure as the mediating variable to explore the contradiction between the influencing factors of the privacy paradox and privacy behaviour, which can clarify the explanatory power of the privacy paradox model used in this study.

2.2. Privacy Calculus Theory. Although the TPB model can help predict people's behavioural intentions and actual behaviours, it cannot ascertain whether incentives or disincentives influence individuals' attitudes. However, PCT can be used to solve this problem. PCT is an important theoretical framework used to study information privacy. It examines the advantages and disadvantages of information disclosure [24]. PCT was first proposed by Laufer and Wolfe [25] and is an important approach in the field of privacy decision-making. According to PCT, the choice of disclosing private information depends on the user's calculation of perceived risks and benefits. When the perceived benefits outweigh the risks, users choose to disclose information. Since this theory was proposed, many scholars have expanded its content. Dinev and Hart [26] adopted PCT in relation to trust, interest, and privacy concerns in order to determine whether users are willing to use the Internet. In recent years, studies have added personalisation [27], convenience [28], and other factors based on the original theory.

This study takes privacy concern, perceived risk, perceived benefit, and trust as inputs for privacy computing and discusses their influence on the college students' intention of disclosing privacy in the context of shared mobility.

2.3. Construal Level Theory. CLT deems that psychological distance influences individuals' intention towards future events by influencing the level of interpretation [29]. In early research on CLT, Liberman and Trope [30] proposed time distance theory wherein the interpretation level of the

distant future, essential, central, and abstract is defined as high level construal, while near future, peripheral, and specific interpretation level is defined as low level construal. Although time distance plays an extremely important role, it is not the only dimension that reflects the level of interpretation. Thus, in the development of CLT, spatial distance [31], social distance [32], and possibility [33] have been proposed as dimensions of CLT. In terms of privacy issues of shared travel users, people tend to represent events that occur in the long-term future, with distant spatial locations, with nonself as the main character or with low probability of occurrence with a high interpretation level psychologically. In other words, users will understand these events in a more abstract and essential way. Conversely, people tend to represent things or events that are near in terms of psychological distance with a low explanatory level and as having more important influence on the near future, spatial distance, and self-themed or more-likely-to-happen events. Therefore, the cognitive mode of the object of CLT can be used to explain why people choose to disclose their private information even in the face of privacy concerns, which further strengthens the explanatory power of the model [34]. However, CLT has rarely been verified or used in the field of privacy paradox. Hallam and Zanella [34] were the first to use CLT to study privacy disclosure behaviour. They added near future and distant future disclosure intentions to their model, using the privacy paradox to explain the impact of perceived benefit on near future disclosure intention, directly affecting their behaviour. In China, He et al. [35] were the first to use the privacy paradox to identify user behaviour from the CLT perspective.

Based on CLT, this study divides disclosure intention into near future disclosure intention and distant future disclosure intention; studies have shown how the four elements of privacy concern, perceived risk, trust (TR), and perceived benefit affect individuals' privacy disclosure intention, affecting privacy disclosure behaviour in turn.

Adopting a review of the literature, this study proposes a relatively complete comprehensive model to examine the privacy paradox of shared mobility in order to integrate TPB, PCT, and CLT. In this model, privacy concern, perceived risk, trust, and perceived benefit affect travellers' near and distant future disclosure intentions, while privacy disclosure intentions ultimately affect users' privacy disclosure behaviours. These factors make this model more explanatory.

3. Research Hypothesis and Theoretical Model

3.1. Privacy Concern. Privacy concern, a common component variable in PCT, measures users' concern regarding personal information. Previous studies have illustrated that users tend to withhold personal information when they are more concerned about privacy [36]. To measure this dimension of privacy concern, Malhotra et al. [37] argued that privacy concern is a multidimensional risk perception, which can be categorised into control, collection, and conscious privacy practices. Subsequently, Hong and Thong [38] refined and expanded the measurement dimensions of privacy concerns and proposed an integrated measurement model. Then, they included and provided measurement standards for collection, secondary use, inappropriate access, error, control, and awareness. Generally, users believe that harm because of privacy disclosure will not happen in the near future or to them. Therefore, the discussion on harm remains at the level of the distant future; that is, the privacy concerns of users inhibit their disclosure intention in the distant future but do not exert significant influence on their disclosure intention in the near future [36].

Thus, this study makes the following assumptions:

H1a: Privacy concerns have a significant negative impact on college students' distant future disclosure intention.

H1b: Privacy concerns have no significant impact on college students' near future disclosure intention.

3.2. Trust. In shared mobility, counterparties are unfamiliar, and transactions should be completed on a platform. Therefore, trust is a key issue that warrants investigation. Moreover, trust is the inherent tendency of an individual to believe another individual based on experience, which can serve as the main driver for user behaviour [39]. Mittendorf [40] categorised trust into two types: trust in drivers and trust in platforms. Additionally, Mcknight et al. [41] grouped trust into three dimensions: integrity, ability, and goodwill. Many studies have demonstrated that users' trust in a platform will influence their intention to disclose information in the near future, because trust will promote the current willingness of a person to disclose information [35].

Therefore, this study makes the following assumptions:

H2a: Trust has a significant and positive impact on college students' near future disclosure intention.

H2b: Trust has no significant impact on college students' distant future disclosure intention.

3.3. Perceived Benefit. Perceived privacy benefit is the driving force for privacy disclosure; it plays an important role in the study of privacy paradox. After providing their personal information, users can obtain rewards, receive bonuses, access services, and gain emotional returns from their counterparty [42]. The dimensions of perceived benefit can be divided into economic incentives, social integration, and personalised services [43]. Users often ignore their privacy concerns for the sake of immediate profit. However, when perceived benefits may exist at a certain future time, owing to uncertainty and other factors, no significant impact is observed. In other words, users' perceived benefits are immediate, and the near term distance grants them a low explanatory level [44].

Therefore, this study makes the following assumptions:

H3a: Perceived benefit has a significant positive impact on college students' near future disclosure intention.

H3b: Perceived benefit has no significant effect on college students' distant future disclosure intention.

3.4. Perceived Risk. In the study of privacy issues, perceived risk is another commonly used variable. It is defined as potential loss perceived by individuals when they disclose information to subjects [37]. Rui [45] examined the willingness of users of social networks to disclose information and found that the greater the perceived risk, the less the willingness of users to disclose private information. In the future, when privacy breaches on ride-sharing platforms occur, users will have a one-sided and hypothetical understanding of the events. Conversely, when users see news reports of privacy breaches, they frequently believe that these incidents will not happen to them or to those around them. Therefore, perceived risk is considered hypothetical, distant, and existing in the distant future [46].

Thus, this study makes the following assumptions:

H4a: Perceived risk has a significant negative impact on college students' distant future disclosure intention.

H4b: Perceived risk has no significant impact on college students' near future disclosure intention.

3.5. Intention and Behaviour of Privacy Disclosure. In TPB, almost all of the factors that affect individual behaviour do so indirectly through individual intention. For CLT, Lynch and Zauberman [29] found that near future disclosure intention placed higher weight on the near future psychological distance than the distant future psychological distance. In other words, users' behaviour is more influenced by near future intentions than distant future intentions.

This study thus makes the following assumptions:

H5a: Near future disclosure intention has a positive impact on privacy disclosure behaviour.

H5b: Distant future disclosure intention has a positive impact on privacy disclosure behaviour.

H5c: The effect of near future disclosure intention on disclosure behaviour is greater than that of distant future disclosure intention.

Finally, we produce the theoretical model shown in Figure 1.

4. Questionnaire Design and Data Collection

4.1. Questionnaire Design. The questionnaire used in this study comprises two parts. The first part collects demographic information, including gender, age, and educational background. The questionnaire features three-dimensional questions for each privacy paradox factor, including privacy concerns, perceived risk, perceived benefit, trust, near future disclosure intention, distant future disclosure intention, and disclosure behaviour. Possible responses to each question range from "completely disagree," "disagree," "uncertain," and "agree" to "completely agree".

In this study, all the variable measurement items involved have been derived from a maturity scale that has been tested in existing studies. To better fit the travel behaviour characteristics of college students regarding shared mobility, we made appropriate adjustments and improvements to the measurement items. Among these items, our study employed the three-dimensional measurement questions in a scale developed by Malhotra [37] for privacy concerns, that by Mittendorf [40] for trust, that by Kehr [47] for perceived benefit, and that by Dinev and Hart [26] for perceived risk. In terms of near future and distant future disclosure intentions, the study utilised the questions designed by Hallam and Zanella [34]. Lastly, the measurement of disclosure behaviour is based on Dienlin and Trepte's [48] investigation of the measurement of privacy disclosure behaviour in the privacy paradox.

4.2. Data Collection. From 3 May to 20 May 2021, this study released the questionnaire online to collect data and used the snowball method to circulate the questionnaire widely. A total of 301 questionnaires were collected. After deleting responses that did not meet the inclusion criteria, 272 valid responses were obtained, with an effective rate of 90.37%.

5. Data Analysis and Results

5.1. Reliability and Validity Analysis. SPSS 24 and Amos 24 software were used to test the reliability and validity of the questionnaire.

Reliability reflects the reliability, stability, and consistency of the questionnaire. In this study, Cronbach's alpha and composite reliability (CR) indexes were used to test the reliability of questionnaires. It is generally considered that Cronbach's coefficient over 0.8 [49] and CR value over 0.7 are good internal consistency levels [50]. The reliability test results are shown in Table 1.

The table indicates that the minimum Cronbach's α value for the seven latent variables is 0.694, which is close to the ideal value of 0.7. On this basis, the minimum value of combined reliability CR is 0.695, which is close to the ideal value of 0.7, indicating that the scale design and measurement model have good reliability.

Validity reflects the validity of the measurement results. The validity test intends to measure whether the questionnaire data can accurately reflect the purpose of the study. In this study, convergent validity and discriminant validity were used to test the validity of data. Generally, the factor loading of the measured variables should be more than 0.7, while the average variance extracted (AVE) should exceed 0.5 to consider the aggregation validity up to the standard. Prior to the validity test, this study conducted factor analysis on the scale. The Kaiser–Meyer–Olkin value of the scale was calculated as 0.791, while Bartlett's sphericity test was significant at the 0.000 level, indicating that the table data were suitable for factor analysis. Tables 1 and 2 present the results of aggregation validity and discriminant validity, respectively. The aggregation validity test indicates that the factor loading of each measurement variable modified in this study is more than 0.565, while the latent variable AVE value is greater than 0.434, indicating that the aggregation degree of the scale is average.

The typical test criterion for discriminating validity is that the square root of the AVE of each potential variable is

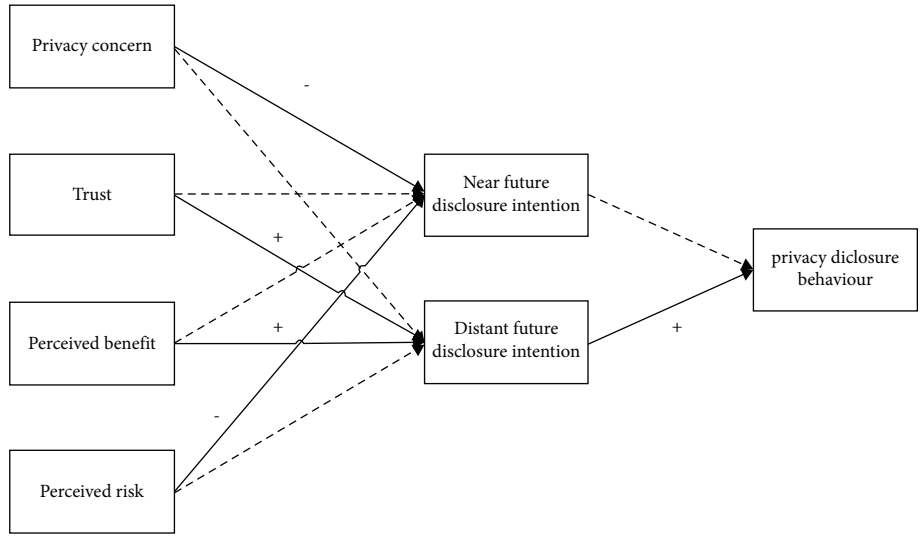

Figure 1: Theoretical model of the shared mobility privacy paradox. Note. Solid line: significant; dashed line: not significant.

Table 1: Reliability and convergent validity tests.

Variable	Questions	Cronbach's alpha	Factor loading	AVE	CR
Privacy concern	Q1a	0.931	0.905	0.822	0.933
	Q1b		0.917		
	Q1c		0.898		
Trust	Q2a	0.887	0.842	0.725	0.888
	Q2b		0.856		
	Q2c		0.856		
Perceived benefit	Q3a	0.694	0.739	0.434	0.695
	Q3b		0.636		
	Q3c		0.592		
Perceived risk	Q4a	0.918	0.836	0.793	0.920
	Q4b		0.943		
	Q4c		0.889		
Distant future disclosure intention	Q5a	0.891	0.903	0.717	0.883
	Q5b		0.802		
	Q5c		0.832		
Near future disclosure intention	Q6a	0.753	0.637	0.495	0.745
	Q6b		0.769		
	Q6c		0.698		
Privacy disclosure behaviour	Q7a	0.758	0.766	0.526	0.765
	Q7b		0.82		
	Q7c		0.565		

greater than the correlation coefficient between it and other potential variables. The measurement results reveal significant differences between potential variables and that the discriminant validity is good.

5.2. Testing of Model Hypothesis. SPSS Statistics 22 and Amos 22 are used to test the proposed model and hypothesis. Table 3 provides the fitting index of the structural model. The simple fit index CMIN/DF, absolute fit indexes AGFI and RMSEA, and value-added fit indexes TLI and CFI reached the fit standard, indicating that the model has a good fit.

Figure 2 shows the path test results of the model.

Table 3 reveals that perceived benefit ($\beta = 0.31$, $p^* = 0.016$) and trust ($\beta = 0.31$, $p^{***} \leq 0.001$) exerted significant positive effects on near future disclosure intention. However, privacy concern ($\beta = -0.05$, $p = 0.239$) and perceived risk ($\beta = -0.07$, $p = 0.193$) had no significant effect on near future disclosure intention. Thus, H1b, H2a, H3a, and H4b are supported. Furthermore, privacy concern ($\beta = -0.34$, $p^{***} \leq 0.001$) and perceived risk ($\beta = -0.29$, $p^{***} \leq 0.001$) exerted significant and negative effects on distant future disclosure intention, respectively. Nevertheless, perceived benefit ($\beta = 0.18$, $p = 0.199$) and trust ($\beta = 0.01$, $p = 0.902$) had no significant effect on distant future disclosure intention, and both are non-significant. These results support H1a, H2b, H3b, and H4a. Ultimately, near future disclosure intention ($\beta = 0.19$, $p^* = 0.021$) exerted a significant positive effect on privacy disclosure behaviour. Distant future disclosure intention

Table 2: Discriminant validity.

	Perceived risk	Perceived benefit	Trust	Privacy concern	Near future disclosure intention	Distant future disclosure intention	privacy disclosure behaviour
Perceived risk	0.890						
Perceived benefit	0.001	0.659					
Trust	0.002	0.014	0.851				
Privacy concern	0.021	0.003	0.002	0.907			
Near future disclosure intention	−0.069	0.077	0.173	−0.079	0.703		
Distant future disclosure intention	−0.308	0.044	0.006	−0.577	0.062	0.847	
privacy disclosure behaviour	−0.034	0.017	0.033	−0.055	0.100	0.077	0.725

Table 3: Fitting index of structural model.

Evaluation indicators	CMIN/DF	RMSEA	AGFI	CFI	TLI
Standard values	<3	<0.08	>0.80	>0.90	>0.90
Measured values	2.456	0.073	0.828	0.917	0.902

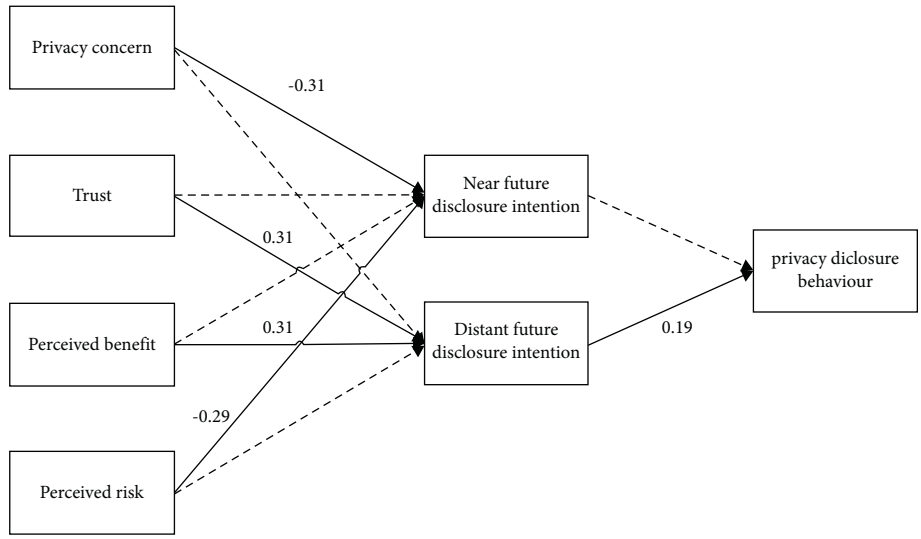

Figure 2: Theoretical model of the shared mobility privacy paradox.

($\beta = 0.07$, $p^* = 0.202$) had no significant effect on privacy disclosure behaviour, and it is nonsignificant. Thus, H5a, H5b, and H5c are supported.

6. Discussion and Conclusions

6.1. Discussion. This study draws the following four conclusions.

First, the privacy paradox does exist in shared mobility. The path test results of the model show that privacy concern only has a significant impact on distant future disclosure intention ($\beta = -0.34$, $p^{***} \leq 0.001$), while near future disclosure intention does not have a significant impact on privacy disclosure behaviour ($\beta = -0.05$, $p = 0.239$), reflecting the contradiction between privacy concern and privacy disclosure behaviour. Based on this conclusion, this study found that privacy concern is at a high explanatory level and only has a significant impact on long-term intention, while long-term intention has no significant impact on behaviour. In other words, although users disclose their personal privacy, they do not reduce their privacy disclosure behaviour. In reality, privacy concern is contrary to privacy disclosure behaviour.

Second, perceived benefit and trust have a significant positive impact on near future disclosure intention, and

perceived benefit is the main inducement factor in near future disclosure intention. Table 3 shows that perceived benefit ($\beta = 0.31$, $p^* = 0.016$) has more influence on near future disclosure intention than trust ($\beta = 0.31$, $p^{***} \leq 0.001$) and the p values for both perceived benefit and trust are less than 0.05. This reflects that college students are more inclined to forgo privacy concerns for certain interests and trust in the platform.

Third, privacy concern and perceived risk have a significant negative impact on college students' distant future disclosure intention, and perceived risk is the main factor affecting it. In Table 3, perceived risk ($\beta = -0.29$, $p^{***} \leq 0.001$) is shown to have a smaller influence on distant future disclosure intention than privacy concern ($\beta = -0.34$, $p^{***} \leq 0.001$).

Finally, both near future and distant future disclosure intentions have positive impacts on privacy disclosure behaviour. Additionally, near future disclosure intention ($\beta = 0.19$, $p^* = 0.021$) has a more significant impact on college students' privacy disclosure behaviour than distant future disclosure intention ($\beta = 0.07$, $p^* = 0.202$). The p value for near future disclosure intention is less than 0.05, while that of distant future disclosure intention is 0.546. This can be explained as follows: according to CLT, because of the existence of time distance, there will be a certain time discount for distant future disclosure intention; thus, its influence is relatively small.

6.2. Countermeasures and Suggestions. This study empirically investigated the privacy paradox and the mechanism of influencing factors in the context of shared mobility and obtained a series of valuable conclusions. To promote the healthy and sustainable development of the shared mobility industry, the following countermeasures and suggestions are proposed for individual users, shared mobility enterprises, and the government.

It is particularly urgent for users to improve their online privacy literacy. The study findings show the phenomenon of the privacy paradox between the privacy concerns and privacy protection behaviours of Chinese shared mobility users—privacy protection behaviours seldom enable the privacy protection consciousness. Studies have shown that one of the main reasons for users' privacy paradox is their lack of knowledge and skilful application of privacy protection tools, that is, online privacy literacy [51]. However, when users understand and master the knowledge and tools of privacy protection, they will no longer be at a loss regarding how to protect their personal privacy from breached [52]. Therefore, improving users' online privacy literacy is greatly important for addressing and preventing privacy leakage problems in shared mobility. Put simply, it is only when the privacy paradox is resolved that users will become more active in shared mobility.

For shared mobility platforms, the key point of optimisation is to improve users' perceived benefits and reduce perceived risks. The study results indicate that perceived benefit is the main promoting factor for privacy disclosure, while perceived risk is the main hindering factor. To improve users' perceived benefit, shared mobility enterprises can optimise platform services and material rewards to satisfy users, such as providing personalised services, increasing the safety and convenience of the platform, and offering discounts. Furthermore, it is extremely important to take technical measures where feasible to improve the privacy protection mechanism in order to reduce the perceived risk of users. Additionally, the platform may make its rules public for information collection and use as well as expressing the purpose, method, and scope of information collection and use in order to strengthen users' ability to control their own information. Finally, platforms itself should abide by professional ethics and prevent the disclosure of personal information to a third party without the consent of users. In other words, the sustainable development of shared mobility platform can be promoted only when users are aware of the benefits brought to them by the platform while also reducing their risk perception.

The government should promote both legislation and practice simultaneously. First, from the legislative viewpoint, although the country has a series of policies and systems in place to restrain the illegal operations of platforms, these are still not sufficiently specific enough. Therefore, regulators should formulate more standardised and detailed privacy policies for shared mobility. From a practical perspective, the education of users and sanctions against illegal platform operations should be strengthened. As aforementioned, only by improving users' privacy literacy level can irrational behaviours, such as excessive panic or excessive vigilance, be avoided. Additionally, the state should also strengthen restrictions and sanctions against the malicious disclosure and the trading of users' private information by service providers on current shared mobility platforms so as to regulate the relevant behaviours of social media platforms and users, reduce privacy risks, and protect users' reasonable willingness to disclose privacy. In other words, only when the state restrains the behaviours of platforms and individuals through legislation and practice can China's shared mobility industry develop in a sustainable and healthy way.

6.3. Limitations and Future Directions. This study investigated the privacy paradox behaviour of college students in the context of shared mobility using a questionnaire survey. We demonstrate that the privacy paradox exists in shared mobility and examine how it is affected by four factors. Our results cast new light on the privacy paradox of shared mobility and provide a good reference for future studies. Furthermore, our results can provide guidance and suggestions for shared mobility platforms. However, several limitations and recommendations for future research can be identified.

To begin with, data collection by online questionnaire cannot achieve truly random sampling, which may affect the research results to some extent. Thus, future research should adopt random sampling and use paper questionnaires. Additionally, although using a questionnaire allows for a wide range of investigations, it cannot fully reflect people's real responses. Therefore, future research will require examining this phenomenon by combining the interview, experimental, and other methods.

	Completely disagree	Disagree	Uncertain	Agree	Completely agree
Q1a: The privacy policy on shared mobility platform should have a clear statement on the use of my personal travel data.	○	○	○	○	○
Q1b: I feel uneasy and worried when a shared mobility platform needs to access my personal information and location information.	○	○	○	○	○
Q1c: When using shared mobility, I take care to provide my personally identifiable information and location information.	○	○	○	○	○

	Completely disagree	Disagree	Uncertain	Agree	Completely agree
Q3a: The cost of disclosing my personal information can be compensated for by shared mobility to let me gain services, convenience, and savings.	○	○	○	○	○
Q3b: I am willing to provide personal information when my friend needs to bargain for a ride on shared transportation.	○	○	○	○	○
Q3c: Shared mobility platforms can provide personalised travel services for me according to my travel preferences.	○	○	○	○	○

	Completely disagree	Disagree	Uncertain	Agree	Completely agree
Q3a: The cost of disclosing my personal information can be compensated for by shared mobility to let me gain services, convenience, and savings.	○	○	○	○	○
Q3b: I am willing to provide personal information when my friend needs to bargain for a ride on shared transportation.	○	○	○	○	○
Q3c: Shared mobility platforms can provide personalised travel services for me according to my travel preferences.	○	○	○	○	○

	Completely disagree	Disagree	Uncertain	Agree	Completely agree
Q4a: I am well aware of the relevant privacy protection provisions when registering on and using shared mobility platforms.	○	○	○	○	○
Q4b: I think that the data on my trip that are recorded by shared mobility platforms will be improperly used.	○	○	○	○	○
Q4c: I think my travel data recorded by shared mobility platforms will bring certain risks.	○	○	○	○	○

	Completely disagree	Disagree	Uncertain	Agree	Completely agree
Q5a: In the future, I will be more cautious about exposing my information on shared mobility platforms.	○	○	○	○	○
Q5b: In the future, I will provide more information inconsistent with my reality on all kinds of shared mobility platforms.	○	○	○	○	○
Q5c: In the future, I plan to reduce travel by shared mobility.	○	○	○	○	○

	Completely disagree	Disagree	Uncertain	Agree	Completely agree
Q6a: I will provide my personal information (including ID card, name, and location information) for the subsidy red envelope granted by shared mobility platform.	○	○	○	○	○
Q6b: I will sign up for this shared mobility app because my friend asked me to help get a red envelope.	○	○	○	○	○
Q6c: I will share good shared mobility app with my friends and family in the near future.	○	○	○	○	○

	Completely disagree	Disagree	Uncertain	Agree	Completely agree
Q7a: I often travel in shared mode, such as shared car, DiDi taxi, and shared bike.	○	○	○	○	○
Q7b: The personal information I fill in on the shared mobility platform is basically consistent with my actual situation.	○	○	○	○	○
Q7c: I fill in a lot of personal information on shared mobility platforms.	○	○	○	○	○

Furthermore, we did not explore the heterogeneity of the privacy paradox among college students. In other words, we did not identify college students' gender, age, or other demographic characteristics. In future research, a differential analysis of surveyed groups can be conducted, which can provide specific suggestions for shared mobility companies to adopt different strategies for different groups.

Finally, this study was mainly aimed at college students, and it should be examined whether the research conclusions can apply to other groups. In the future, the scope of the survey sample can be expanded to improve the robustness and applicability of the model.

Appendix

A Study on the Privacy Paradox in China's Shared Mobility

Hello! First, thank you for reading and filling in this questionnaire in your busy schedule! This questionnaire is conducted anonymously and will take about 3–5 minutes. The purpose of the survey is to discuss the privacy paradox in China's shared travel. There is no right or wrong answer; please choose the one that fits your situation. The results will only be used for academic research and will never involve commercial content or divulge personal privacy. Thank you again for your support and cooperation!

1. Gender [single choice] *

A. Male
B. Female

2. Your age [single choice] *

A. Under the age of 18
B. 19–25 years old
C. 26–35 years old
D. Age 35 and above

3. Degree [single choice] *

A. High school and below
B. College
C. Bachelor degree
D. Master's degree or above

4. Privacy concerns (Matrix scale questions) [Matrix multiple choice questions] *.

5. Trust (Matrix scale questions) [Matrix multiple choice questions] *.

6. Perceived benefits (Matrix scale questions) [Matrix multiple choice questions] *.

7. Perceived risk (Matrix scale questions) [Matrix multiple choice questions] *.

8. Distant future disclosure intention (Matrix scale questions) [Matrix multiple choice questions] *.

9. Near future disclosure intention (Matrix scale questions) [Matrix multiple choice questions].

10. Privacy disclosure behaviour (Matrix scale questions) [Matrix multiple choice questions] *.

Data Availability

Data from the survey-based questionnaire, which were used to support the findings of this study, are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This paper was jointly supported by the Chinese National Natural Science Foundation (61803314) and the Young Scholars Fund of Xihua University.

References

[1] K. Turon, P. Czech, and J. Toth, "Safety and security aspects IN shared mobility systems," *Sci. J. SILESIAN Univ. Technol. Transp.*vol. 104, pp. 169–175, 2019.

[2] "Sharing Economy Research Center of State Information Center Releases Sharing Accommodati on Service Standard," [Online]. Available: http://www.sic.gov.cn/News/568/10429.htm, November 2018.

[3] "Statistical Survey Report on Internet Development in China," 2021, http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/.

[4] "Notification on the Removal of 25 Apps Including Didi Enterprise Edition," July 2021, http://www.cac.gov.cn/2021-07/09/c_ 1627415870012872.htm.

[5] "Ministry of Industry and Information Technology: Notification ofAPP Infringement of User Ri Ghts and Interests," The 10th Batch of the 1st Batch in 2021, November 2019.

[6] B. van der Sloot, "A new approach to the right to privacy, or how the European Court of Human Rights embraced the non-domination principle," *Computer Law & Security Report*, vol. 34, no. 3, pp. 539–549, 2018.

[7] B. Toader, A. Moawad, T. Hartmann, and F. Viti, "A data-driven scalable method for profiling and dynamic analysis of shared mobility solutions," *Journal of Advanced Transportation*, vol. 2021, pp. 1–15, 2021.

[8] S. B. Barnes, "A privacy paradox: social networking in the United States," *First Monday*, vol. 11, no. 9, 2006.

[9] A. M. Zafeiropoulou, D. E. Millard, C. Webber, and K. O'Hara, "Unpicking the privacy paradox: can structuration theory help to explain location-based privacy decisions?" *Proc. 5th Annu. WebSci'13*, vol. 21, pp. 463–472, 2013.

[10] H. Krasnova, N. F. Veltri, and O. Günther, "Self-disclosure and privacy calculus on social networking sites: the role of culture," *Business & Information Systems Engineering*, vol. 4, no. 3, pp. 127–135, 2012.

[11] R. A. Bauer, "Consumer Behavior as Risk Taking," in *Proceedings of the 43rd. Conference of the American Marketing Association*, pp. 389–398, June 1960.

[12] Q. Chen, H. Zhang, J. Wang et al., "Impact of shared Bus on campus travel and space optimization based on activity travel behavior," *Journal of Advanced Transportation*, vol. 2021, pp. 1–18, 2021.

[13] L. Rotaris, R. Danielis, and I. Maltese, "Carsharing use by college students: the case of Milan and Rome," *Transportation Research Part A: Policy and Practice*, vol. 120, pp. 239–251, 2019.

[14] A. Arm, A. Tods, A. Hnp, A. Adpds, B. Tdds, and A. Pdles, "Guidelines to design bicycle routes on university campuses: a case study at the Federal University of Viosa," *Case Stud. Transp. Policy*, vol. 8, no. 2, pp. 620–626, 2020.

[15] J. Christopher, M. Armitage, and Conner, "Efficacy of the theory of planned behaviour: a meta-analytic review," *British Journal of Social Psychology*, vol. 40, no. 4, pp. 471–499, 2001.

[16] I. Ajzen, "Attitudes, traits, and actions: dispositional prediction of behavior in personality and social psychology," *Advances in Experimental Social Psychology*, vol. 20, pp. 1–63, 1985.

[17] M. Conner, P. Norman, and R. Bell, *The Theory of Planned Behavior and Healthy Eating*, Health Psychol., 2002.

[18] S. Shim, M. A. Eastlick, S. L. Lotz, and P. Warrington, "An Online Prepurchase Intentions Model: The Role of Intention to Search," *J. Retail.*vol. 77, 2001.

[19] M. Akulume and S. N. Kiwanuka, "Health Care Waste Segregation Behavior among Health Workers in Uganda: An Application of the Theory of Planned Behavior," *J. Environ. Public Health*, vol. 2016, Article ID 8132306, 8 pages, 2016.

[20] L. H. Yang, X. Q. Zhang, X. Y. Zhu, Y. L. Luo, and Y. Luo, "Research on risky driving behavior of novice drivers," *Sustainability*, vol. 1120 pages, 2019.

[21] I. Luiza, L H. Matsunaga, C. C. Machado et al., "Psychological determinants of walking in a Brazilian sample: an application of the Theory of Planned Behavior," *Transp. Res. PART F-TRAFFIC Psychol. Behav.*vol. 73, pp. 391–398, 2020.

[22] B. Imani, M. S. Allahyari, A. Bondori, J. Surujlal, and B. Sawicka, "Determinants of organic food purchases intention: the application of an extended theory of planned behaviour," *Futur. FOOD-JOURNAL FOOD Agric. Soc.*vol. 9, no. 1, pp. 18–29, 2021.

[23] M. O. Lwin and J. D. Williams, "A model integrating the multidimensional developmental theory of privacy and theory of planned behavior to examine fabrication of information online," *Marketing Letters*, vol. 14, no. 4, pp. 257–272, 2003.

[24] T. Nguyen, "Continuance intention in traffic-related social media: a privacy calculus perspective," *Journal of Internet Commerce*, vol. 20, no. 2, pp. 215–245, 2021.

[25] R. S. Laufer and M. Wolfe, "Privacy as a concept and a social issue: a multidimensional developmental theory," *Journal of Social Issues*, vol. 33, no. 3, 1977.

[26] T. Dinev and P. Hart, "Internet privacy concerns and their antecedents - measurement validity and a regression model," *Behaviour & Information Technology*, vol. 23, no. 6, pp. 413–422, 2004.

[27] A. Gutierrez, S. O'Leary, N. P. Rana, Y. K. Dwivedi, and T. Calle, "Using privacy calculus theory to explore entrepreneurial directions in mobile location-based advertising: identifying intrusiveness as the critical risk factor," *Computers in Human Behavior*, vol. 95, no. JUN, pp. 295–306, 2019.

[28] H. Krasnova, S. Spiekermann, K. Koroleva, and T. Hildebrand, "Online social networks: why we disclose," *Journal of Information Technology*, vol. 25, no. 2, pp. 109–125, 2010.

[29] J. Lynchjr and G. Zauberman, "Construing consumer decision making," *Journal of Consumer Psychology*, vol. 17, no. 2, pp. 107–112, 2007.

[30] N. Liberman and Y. Trope, "The role of feasibility and desirability considerations in near and distant future decisions: a test of temporal construal theory," *Journal of Personality and Social Psychology*, vol. 75, no. 1, pp. 5–18, 1998.

[31] L. Jia, E. R. Hirt, and S. C. Karpen, "Lessons from a faraway land: the effect of spatial distance on creative cognition," *Journal of Experimental Social Psychology*, vol. 45, no. 5, pp. 1127–1131, 2009.

[32] E. Stephan, N. Liberman, and Y. Trope, "Politeness and psychological distance: a construal level perspective," *Journal of Personality and Social Psychology*, vol. 98, no. 2, pp. 268–280, 2010.

[33] C. J. Wakslak, Y. Trope, N. Liberman, and R. Alony, "Seeing the Forest when Entry Is Unlikely: Probability and the Mental Representation of Events," *Journal of Experimental Psychology: General*, vol. 135, no. 4, pp. 641–653.

[34] C. Hallam and G. Zanella, "Online self-disclosure: the privacy paradox explained as a temporally discounted balance between concerns and rewards," *Computers in Human Behavior*, vol. 68, pp. 217–227, 2017.

[35] L. He, Y. Lu, Y. Xu, M. Xie, S. O. Management, and J. University, "Research on privacy paradox in social network sites under the perspective of construal level theory," *Journal of the China Society for Scientific and Technical Information*, vol. 37, no. 1, pp. 1–13, 2018.

[36] L. Nemec Zlatolas, T. Welzer, M. Heričko, and M. Hölbl, "Privacy antecedents for SNS self-disclosure: the case of Facebook," *Computers in Human Behavior*, vol. 45, pp. 158–167, 2015.

[37] N. K. Malhotra, S. S. Kim, and J. Agarwal, "Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model," *Information Systems Research*, vol. 15, no. 4, pp. 336–355, 2004.

[38] W. Hong and J. Thong, "Internet privacy concerns: an integrated conceptualization and four empirical studies," *MIS Quarterly*, vol. 37, no. 1, pp. 275–298, 2013.

[39] X. Xie, T. Niannchung, Z. Huang, W. Wu, and S. O. Management, *Investigation of Determinants of Social Media User Privacy Paradoxical Behavior*, Libr. Inf. Serv., 2018.

[40] C. Mittendorf, "The implications of trust in the sharing economy–An empirical analysis of Uber," *in Proceedings of the 50th Hawaii International Conference on System Sciences*, vol. 59, 2017.

[41] D. H. Mcknight, V. Choudhury, and C. Kacmar, "Developing and validating trust measures for e-commerce: an integrative typology," *Information Systems Research*, vol. 13, no. 3, pp. 344–359, 2002.

[42] A. Alessandro, J. K. Leslie, and L. George, "What is privacy worth?" *The Journal of Legal Studies*, vol. 42, 2013.

[43] E. F. Stone and L. D. Stone, "Privacy in organizations: theoretical issues, research findings, and protection mechanisms," *Research in Personnel and Human Resources Management*, vol. 8, 1990.

[44] H. Zhu, K. Wang, Z. Yan, and J. Wu, "An analysis of privacy paradox phenomenon in SNS users based on privacy calculus," *Journal of Intelligence*, vol. 36, no. 2, pp. 134–140, 2017.

[45] C. Rui, "Living a private life in public social networks: an exploration of member self-disclosure," *Decision Support Systems*, vol. 55, no. 3, pp. 661–668, 2013.

[46] C. Lutz and P. Strathoff, "Privacy concerns and online behavior – not so paradoxical after all? Viewing the privacy paradox through different theoretical lenses," *Multinationale Unternehmen und Institutionen im Wandel – Herausforderungen für Wirtschaft*, Recht und Gesellschaft, Berlin, Germany, 2013.

[47] F. Kehr, T. Kowatsch, D. Wentzel, and E. Fleisch, "Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus," *Information Systems Journal*, vol. 25, no. 6, pp. 607–635, 2015.

[48] T. Dienlin and S. Trepte, "Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors," *European Journal of Social Psychology*, vol. 45, no. 3, 2015.

[49] J. F. Hair, W. C. Black, B. J. Babin, and R. E. Anderson, "Multivariate data analysis: a global perspective," *Loan/open Shelves*, vol. 4, 2014.

[50] R. P. Bagozzi, "Evaluating structural equation models with unobservable variables and meas error: a comment," *Journal of Marketing Research*, vol. 18, 1981.

[51] A. E. Waldman, "There is No privacy paradox: how cognitive biases and design dark patterns affect online disclosure," *Curr. Opin. Psychol.*vol. 31, 2019.

[52] S. Trepte, D. Teutsch, P. K. Masur, C. Eichler, and F. Lind, *Do People Know about Privacy And Data Protection Strategies? Towards The "Online Privacy Literacy Scale" (OPLIS)*, Reforming Euro-pean Data Protection Law, Netherland, 2015.