Journal of
Theoretical and Applied Electronic Commerce Research

MDPI

Article

How Can Users Be Confident About Self-Disclosure in Mobile Payment? From Institutional Mechanism Perspective

Haiqin Xu and Jian Li *

School of Business, Anhui University, Hefei 230601, China; hqxu@ahu.edu.cn
* Correspondence: lijian91@ahu.edu.cn

Abstract

Mobile payment platforms not only streamline users' financial transactions but also encourage their participation in investment activities and additional services. To deliver personalized financial services, it is essential to collect users' personal information. This study aims to investigate the factors influencing users' willingness to engage in self-disclosure within mobile payment platforms, thereby assisting practitioners in efficiently allocating resources and maximizing returns on investments dedicated to promoting user self-disclosure. Consequently, this study focuses on examining how institutional mechanisms influence users' self-disclosure behavior within these platforms. The authors developed a comprehensive framework that elucidates the influence of institutional mechanisms on users' self-disclosure, mediated by trust and privacy concerns. To empirically validate our research model, we administered an online survey targeting Alipay users in China. Subsequently, we analyzed 559 valid survey responses utilizing partial least squares structural equation modeling (PLS-SEM). The results indicate that trust and privacy concerns jointly influence users' self-disclosure behavior when utilizing mobile payment platforms. Moreover, key institutional mechanisms can effectively foster trust and alleviate privacy concerns, ultimately facilitating users' willingness to self-disclose. Our research shifts scholarly focus from conventional adoption to users' self-disclosure in the mobile payment field and enhances the existing self-disclosure research by identifying the impact of institutional mechanisms on users' self-disclosure behavior.

Keywords: institutional mechanisms; self-disclosure; information privacy; mobile payment

1. Introduction

Mobile payment, a legally regulated financial service, has witnessed a remarkable surge in popularity over the past decade. Because of the large market potential, serval mobile payment apps have emerged, including Apple Pay, PayPal, Android Pay, Alipay Wallet, and WeChat Wallet [1]. Mobile payments apps are used by more than two billion individuals globally, with millions more coming each year (https://www.businessofapps.com/data/mobile-payments-app-market/, accessed on 25 September 2025). Recently, 53% of UK consumers have opted for products online via PayPal, while 30% have chosen Apple Pay (https://www.emarketer.com/content/uk-digital-wallets-2024, accessed on 25 September 2025). In order to supply users with meticulously designed financial services, mobile apps frequently collect and utilize a range of personal information from users [2]. Simultaneously, the collecting and usage of personal information have raised users' concerns regarding information privacy, potentially impeding their use of mobile payment apps. Approximately 56% of users in China explicitly express apprehension about data

Check for updates

Academic Editor: Ting Chi

Received: 3 October 2025
Revised: 17 December 2025
Accepted: 18 December 2025
Published: 1 January 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

security and are hesitant to share their private data when using mobile payment apps (https://www.iimedia.cn/c1061/103479.html, accessed on 25 September 2025). Therefore, an ongoing challenge in the mobile payment industry is to alleviate users' privacy concerns and promote self-disclosure in mobile payment apps.

Previous researchers have enhanced our comprehension of the elements influencing users' self-disclosure in online environments. We would like to emphasize two areas that necessitate further examination. First, the existing literature on self-disclosure primarily focuses on business and social technology environments, including online platforms and social networking sites [3–5]. However, financial technology, including mobile payment apps, has been largely overlooked despite being one of the most sensitive areas for information leakage and data breaches [6]. There's a tug-of-war between providers leveraging clients' private data to provide advantageous and customized financial offerings and the mounting worries of consumers regarding information privacy, and this can inhibit consumers' willingness to disclose private information to mobile payment apps. Thus, understanding users' self-disclosure in mobile payment holds both theoretical as well as practical value. In theory, this provides a possibility to alter the existing focus of self-disclosure studies from social network contexts to economic technology contexts. The findings could assist scholars in specifying conditions under which users are more likely to disclose their personal financial information and direct future research to examine self-disclosure issues in other financial technologies that include crowdfunding, digital currency, and peer-to-peer lending. Practically, a comprehensive understanding of self-disclosure in mobile payment apps can guide practitioners in effectively allocating resources and optimizing returns on investments made towards promoting users' self-disclosure.

Second, the existing self-disclosure research has paid minimal attention to the role of institutional mechanisms on self-disclosure. Existing studies have predominantly focused on individual psychological factors, such as emotional state [7], self-presentation [8,9], and perceived convenience [5], and social psychological factors, including social influence [10], and social rewards [5], and social presence [3]. A more fundamental category of drivers, institutional mechanisms, which indicate the impersonal safeguards present in the online transaction environment that aim to mitigate transactional risks and ensure successful transactions when using mobile payment apps, has been largely overlooked in the existing literature. Given the risk and uncertainties in online transactions, institutional mechanisms may effectively protect users' private data from unlawful use and access, thereby influencing their willingness to disclose personal information [11]. This study seeks to systematically examine how various institutional mechanisms collectively influence users' self-disclosure behaviors and offers actionable insights for practitioners and regulators aiming to foster a safer and more trustworthy mobile payment ecosystem through comprehensive institutional design, rather than relying solely on technical solutions or psychological interventions.

Motivated by this challenge in self-disclosure research, we have established a model to account for the effects of institutional mechanisms upon users' self-disclosure in mobile payment apps. Drawing upon existing literature on self-disclosure, we claim that self-disclosure in mobile payment apps is an interplay between users' trust and privacy concerns. We argue that the institutional mechanisms effectively facilitate users' self-disclosure by establishing trust and addressing privacy concerns. We empirically examine our research model using a sample of 559 Alipay Wallet users who had experience with this popular mobile payment app. The findings strongly support our research model and give a solid framework for subsequent research on self-disclosure.

2. Theoretical Background

2.1. Mobile Payment

Previous research concerning mobile payment has generally focused on exploring factors related to customers' adoption behavior, retention behavior, switching behavior, and loyalty to mobile payment (refer to Table S1 in Supplementary Material). For example, several studies have shown that performance expectancy, effort expectancy, social influence, facilitating conditions, trusting beliefs, structural assurance, and privacy risks collectively formulate users' loyalty to mobile payment apps [11,12]. Consistent with innovation diffusion theory [13], some scholars have proposed that relative advantage, compatibility, visibility, trusting beliefs, privacy risks, and perceived costs influence users' propensity to employ mobile payment apps. Summarizing this research, we have observed that limited attention has been given to self-disclosure in mobile payment apps within the existing literature on mobile payment [14].

2.2. Self-Disclosure

Prior studies have primarily examined the psychological processes and antecedents that affect users' self-disclosure in online environments (refer to Table S2 in Supplementary Material). These studies can be broadly categorized into two streams. The first stream examines motivators that encourage users to self-disclose, such as trust [3,15], perceived benefits [16], privacy assurance approaches [17], emotional state [7], and affective commitment [18]. Trust, which refers to users' cognitive beliefs that online companies have attributes that they can rely on in handling their personal information, is one of the most often researched motivators pertaining to users' self-disclosure in the IS discipline [15]. Since the process of exchanging information is characterized by uncertainty, interdependence, and fear of opportunism, trust is essential to its governance. Trust may help users disclose more about themselves by reducing uncertainties and risks during the information exchange process [3].

The second line of research focuses on identifying barriers that prevent users from disclosing personal information to others. These barriers include privacy concerns [19–21], perceived intrusiveness to information boundary [20], perceived invasion [19], privacy risks [16], and perceived information sensitivity [19]. Privacy concerns have been extensively examined by the IS discipline as a major issue influencing users' unwillingness to divulge personal information [22]. Privacy concerns refer to the apprehensions users have regarding potential privacy breaches resulting from sharing their information [23]. Privacy concerns can inhibit users' self-disclosure because they often worry about unauthorized collection and storage of their personal data in databases or its potential secondary use without proper consent from users [23]. Despite previous studies identifying various motivators and inhibitors for disclosing personal information, the impact of institutional mechanisms on users' self-disclosure has been largely neglected.

2.3. Institutional Mechanisms

According to Pavlou & Gefen (2004), institutional mechanisms are impersonal institutions implemented by internet providers or third-party associations to mitigate transaction risks and ensure successful transactions [24]. Fang et al. (2014) proposed a two-dimensional taxonomy to account for institutional mechanisms [25]. The first dimension captures the level of application specificity, while the second represents the degree of negative risk framing. This taxonomy further yields four types of institutional mechanisms [11] (see Figure 1): (I) general structural assurance, (II) general institutional structure, (III) local structure assurance, and (IV) local institutional structure (refer to Table S3 in Supplementary Material).

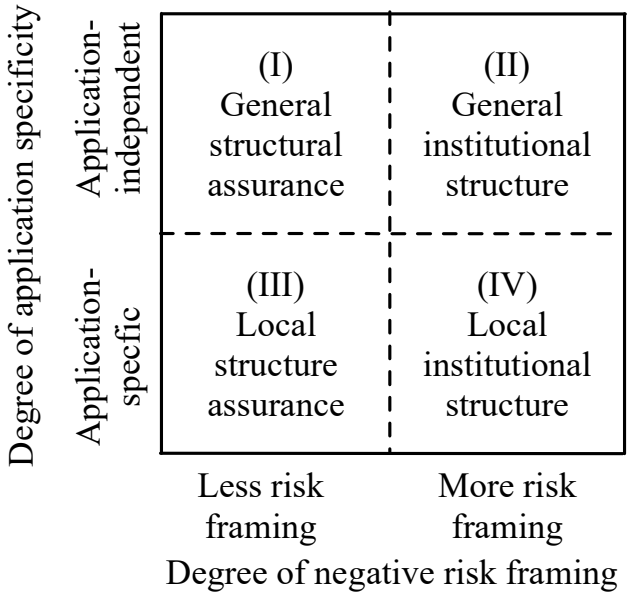


Figure 1. Topology of Institutional Mechanism in [11].

The two-dimensional topology suggests that (I) and (II) are application-independent institutional mechanisms [11]. These mechanisms are derived from robust safeguards on the Internet that transcend any mobile application. Regarding mobile payment apps, (I) and (II) encompass government legislation pertaining to the mobile payment industry, technological innovations in mobile payment infrastructures, and the maturity level of the mobile payment marketplace [26]. The contextual risks in online transaction environments that are outside the control of individual mobile payment apps can be mitigated by these application-independent institutional mechanisms [27]. In contrast to (I) and (II), (III) and (IV) are application-specific institutional mechanisms that effectively establish trust and mitigate risks inherent in transactional relationships with a particular mobile application [28]. Within the context of mobile payment apps, these mechanisms encompass various in-application safeguards such as user profile technologies, rating and feedback systems, escrow services, and privacy compensation policies [29]. These application-specific institutional mechanisms serve to protect users from data breaches or personal information leaks during financial payment service usage.

Although (I), (II), (III), and (IV) possess the capability to mitigate risk in the online transaction environment, they vary in how much negative risk framing they employ [25]. Structural assurances such as (I) and (III) focus on the effect of institutional mechanisms on security/success assurance. For instance, Pavlou Gefen [24] suggested that feedback mechanisms, escrow services, and credit card guarantees are appropriate institutional mechanisms for ensuring transactional success. Gefen et al. reported that guarantees, regulations, promises, and legal resources are effective institutional mechanisms implemented to promote successful online transactions [30]. On the contrary, institutional structures like (II) and (IV) revolve around the role of institutional mechanisms in risk mitigation. For instance, institutional mechanisms are clearly described by Fang et al. as safeguards that exist in the e-commerce ecosystem to protect users from potential hazards in online transactions [25].

There are three theoretical distinctions among these four institutional mechanisms. First, based on cue utilization theory, users' perception of product quality stems from both internal and external cues [31,32]. General institutional mechanisms, such as (I) and (II), are external cues derived from the macro environment outside the platform and provide an important external reference system for users to assess the platform. However, they are

not part of the platform's products or services themselves. Local institutional mechanisms, such as (III) and (IV), are internal cues—specific functions and service commitments that platform developers deliberately design and embed within the application. Second, based on trust transfer theory [12], individuals' trust in an unfamiliar object can be transferred from a related object they already trust. General institutional mechanisms such as (I) and (II) focus on the macro-environment of the industry. Trust based on general institutional mechanisms is typically transferred from trust in the macro-environment. In contrast, trust based on local institutional mechanisms such as (III) and (IV) does not rely on external sources but represents an endogenous process of directly building trust within the platform. Third, according to regulatory focus theory [33], human behavior is driven by two distinct motivational systems: promotion focus, which centers on growth and attainment, and prevention focus, which focuses on safety and responsibility and involves avoiding loss. All four of these institutional mechanisms serve the prevention focus, but there are still some distinctions among them. Structural assurances such as (I) and (III) mainly operate at the level of process security. By demonstrating technical capabilities and process robustness, they are committed to minimizing the probability of risk occurrence. In contrast, institutional structures such as (II) and (IV) act at the level of consequence security. They are committed to minimizing the losses after risks occur.

More specifically, (I) and (II) offer a sense of security that is distant and based on background information, whereas (III) and (IV) provide a sense of security that is close and context-based. Meanwhile, (I) and (III) primarily address users' doubts regarding the ability of the mobile payment industry or platform to protect them, while (II) and (IV) mainly respond to the more profound concerns about whether the mobile payment industry or platform is willing to protect them and take action in case of problems. For example, when someone is contemplating using Alipay's financial services, which necessitate the disclosure of personal information and the assumption of financial risks, four institutional mechanisms come into play in influencing the decision: (I) General structural assurance. The individual has a vague belief that "the government strictly regulates financial apps, and Alipay won't be fraudulent software," which provides a fundamental sense of security. (II) General institutional structure. The person thinks of the "Personal Information Protection Law" and believes that the platform will not casually disclose their loan information, thereby obtaining general regulatory guarantees. (III) Local structural assurance. The security prompt on the activation page instills trust in Alipay's technical capabilities, motivating the individual to take further steps. (IV) Local institutional structure. The commitment in the terms stating that "If an account is stolen and non-own borrowing occurs, it will be 100% compensated after verification" completely dispels the individual's concerns and enables them to finally make a decision.

3. Research Model and Hypotheses

In order to take into consideration the impact of institutional mechanisms on consumer self-disclosure behavior, we have developed a research model, which is shown in Figure 2. Drawing on the self-disclosure literature, we first propose that consumers' self-disclosure is an interplay of their trust and privacy concern toward privacy information disclosure. Then, following the institutional mechanism literature, we propose that these institutional mechanisms can effectively increase consumer trust and reduce their privacy concerns regarding information disclosure. Finally, we include age, gender, education, income, usage experience, and usage frequency as control variables in the model.

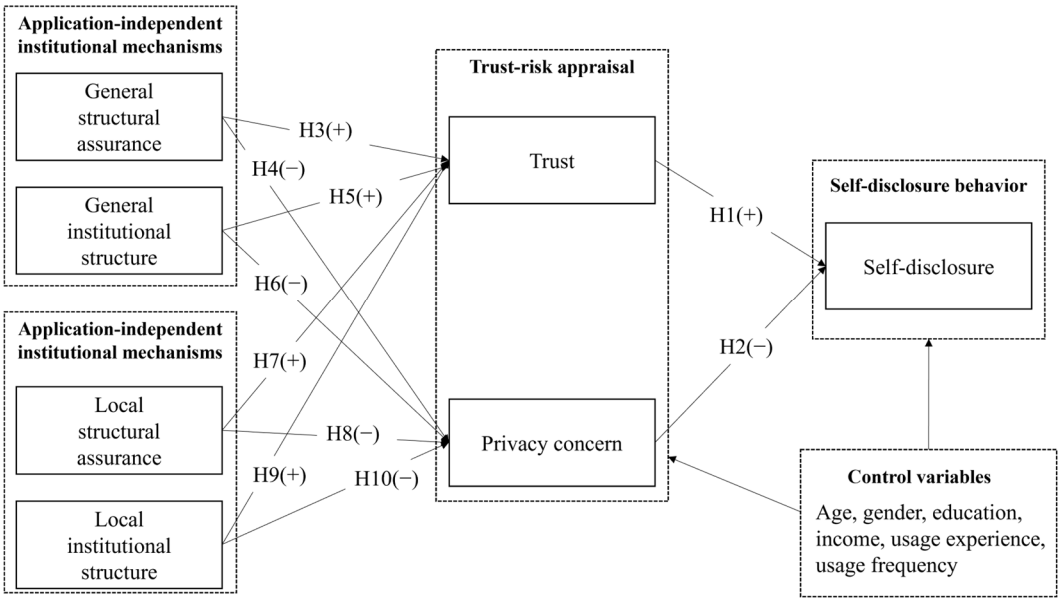


Figure 2. Research model.

3.1. Trust-Risk Appraisal and Self-Disclosure Behavior

It is commonly known that trust is related to the behavior intention. Additionally, it has been demonstrated that trust has a favorable impact on individuals' willingness to divulge private information in a variety of research situations, including online health communities [7], e-commerce [34], and social networking sites [3]. If consumers believe their given information is adequately protected, they are more inclined to have a high degree of trust in the mobile payment setting, and users are therefore more willing to divulge information through mobile payment apps. As a result, consumers are encouraged to divulge personal information with confidence due to the increased degree of trust in mobile payment apps. Consequently, we postulate the following:

H1. *Self-disclosure behavior is positively correlated with trust.*

Numerous research contexts, such as online health communities [7], e-commerce [34], and social networking sites [3], have shown the negative impacts of privacy concerns on individuals' willingness to divulge personal information. Data gathering, unauthorized secondary use, errors, and improper access to personal information are some of the components of organizational opportunistic behavior that have been revealed by previous privacy research [35]. Therefore, privacy concern is a major factor in inhibiting self-disclosure. Similarly, users of mobile payments also exhibit substantial concerns regarding information disclosure due to potential negative consequences like financial risk and privacy risk. As a result, it is anticipated that consumers who are more concerned about their privacy may disclose less on mobile payment apps. Consequently, we postulate the following:

H2. *Self-disclosure behavior is negatively correlated with privacy concern.*

3.2. General Structural Assurance and Trust-Risk Appraisal

General structural assurance refers to the degree to which mobile payment users believe that legal protections and technological Internet safeguards assure them that transactions with mobile payment are secure [36]. The legal protections make each transaction partner's behavior predictable and set punitive costs for inappropriate behaviors higher than the benefits of violating contractual stipulations [37]. Technology safeguards are the

technological infrastructures built into mobile payment apps that ensure secure payment process [28]. Examples of these include data storage techniques, encryption technology, password protection, etc. [38]. Both legal protections and technology safeguards are designed to create a safer environment for mobile payment users, enhancing trust beliefs and alleviating privacy concerns.

Previous privacy literature has shown that general structural assurance has a role in mitigating privacy concerns and enhancing trust. For instance, Zhou (2012) indicated that structural assurance is positively related to initial trust [26]. Additionally, Shao et al. (2022) revealed that structural assurance of internet has a large and detrimental effect on privacy risk in the e-government environment [36]. Within the present study conducted in a mobile payment setting, we consider general structural assurance as defined at a general level and framed to emphasize its function in providing protection and reassurance, which is likely to foster trusting beliefs and reduce privacy concerns. Consequently, we postulate the following:

H3. *Trust is positively correlated with general structural assurance.*

H4. *Privacy concern is negatively correlated with general structural assurance.*

3.3. General Institutional Structure and Trust-Risk Appraisal

The general institutional structure refers to the overall descriptions regarding the presence of safeguards (such as third-party certifications and credit card guarantees) in the mobile payment environment, which aim to protect them from potential risks related to employment in mobile payment services [25]. This concept clearly frames the overall institutional framework in terms of risk mitigation. Accordingly, it focuses on creating a secure payment environment by addressing privacy concerns with clear regulatory assurances [25]. Various trusted third-party seals have been introduced to alleviate consumer privacy concerns in the online context [39]. These third-party assurance seals assure users that their online services meet industry standards and guarantee a minimum level of service quality.

Prior research on privacy has demonstrated the significant role of general institutional structure in fostering trust and mitigating privacy concerns. For example, assurance seals effectively reduce privacy concerns within the e-commerce environment [39]. According to trust transfer theory [36], users might extend their trust in these third parties to mobile payment apps. Therefore, users' initial trust in mobile payment apps may be impacted by general structural assurance. Consequently, it can be argued that general structural assurance plays a crucial role in shaping users' trust and addressing privacy concerns. Considering previous investigations, our study posits that an overarching institutional structure defined at a general level and framed to emphasize contextual risk mitigation can have significant implications for enhancing trusting beliefs and alleviating privacy concerns. Consequently, we postulate the following:

H5. *Trust is positively correlated with general institutional structure.*

H6. *Privacy concern is negatively correlated with general institutional structure.*

3.4. Local Structural Assurance and Trust-Risk Appraisal

The concept of local structural assurance pertains to the extent to which users of mobile payment perceive that the apps' legal and technological safeguards ensure secure transactions [28]. Mobile payment apps can mitigate information privacy concerns and enhance trust regarding the security and privacy of their technological infrastructure and legal [28]. If mobile payment users lack confidence in the efficacy of structural assurance in establishing

appropriate rules within the internet environment, application-specific structural assurance becomes necessary to bolster their confidence in using mobile payment apps [25].

As an effective mechanism is built into specific online service providers, local structural assurance is utilized to boost confidence and reduce privacy concerns. For instance, Srivastava & Chandra (2018) revealed that the structural assurance of the virtual world can enhance user trust in the virtual world [40]. Researchers had demonstrated that the structural assurance of online banking system has a favorable influence on consumer trust [28]. Additionally, previous studies on privacy have also shown that trust can alleviate privacy concerns [41]. Building upon these findings, this research posits that local structural assurance, defined at the local level with an emphasis on providing protection and assurances, could play a crucial role in fostering trusting beliefs and mitigating privacy concerns. Consequently, we postulate the following:

H7. *Trust is positively correlated with local structural assurance.*

H8. *Privacy concern is negatively correlated with local structural assurance.*

3.5. Local Institutional Structure and Trust-Risk Appraisal

The local institutional structure refers that the specific mobile payment apps have safeguards, such as privacy policies and guarantees, in place to protect users from potential risks related to using mobile payment services [11]. Unlike the general institutional structure developed by third-party organizations, the local institutional structure is created by specific online service providers [25]. These policies and guarantees elucidate the purpose and intended use of user personal information while communicating their privacy handling policy to users [39]. Consequently, it empowers users to enhance their perceived control over disclosed personal information shared with online service providers. Keeping these factors in mind, the local institutional structure enhances initial confidence among users towards specific online providers due to their desire for protection of their informational privacy.

Prior researchers on privacy have suggested that the local institutional structure is an effective mechanism for building perceived trust and reducing privacy concerns in various contexts. Previous mobile payment research has also shown that the institutional structure provided by service firms contributes positively to the formation of users' initial trust in mobile payment [42]. Mousavizadeh et al. (2016) revealed that assurance statements of e-commerce websites alleviate online users' privacy concerns [39]. Based on these findings, this study suggests that a local institutional structure, defined at the local level and designed to emphasize contextual risk reduction, could have significant implications for enhancing trusting beliefs and mitigating privacy concerns. Consequently, we postulate the following:

H9. *Trust is positively correlated with local institutional structure.*

H10. *Privacy concern is negatively correlated with local institutional structure.*

4. Research Method

In order to perform the empirical validation of our research model, we performed an online survey in China. The target survey population consisted of current users of a popular mobile payment application, specifically Alipay Wallet. The subsequent subsections offer detailed information regarding the research method.

4.1. Research Setting

We selected Alipay Wallet as the research context due to several reasons. Firstly, Alipay Wallet is the predominant mobile payment application in China with a user base exceeding

870 million individuals, ensuring that our data is representative. Secondly, Alipay has obtained certifications from reputable third-party organizations such as PCI-DSS, VeriSign, and Visa. This allows us to examine the influence of general institutional structure within our research model. Thirdly, Alipay Wallet incorporates various protective measures including feedback technologies, user profile technologies, escrow services, and insurance guarantees to establish a secure payment environment. This presents an opportunity for us to explore the role of local structural assurance in our research model. Lastly, Alipay Wallet publishes multiple policies aimed at ensuring safety and security during transactions. This allows us to examine the impact of local institutional structure in our research model. In summary, investigating the role of institutional mechanisms within Alipay Wallet presents a valuable opportunity for our study.

4.2. Data Collection

We employed the widely used online survey platform Sojump to distribute our survey questionnaire. To ensure that respondents completed the questionnaire carefully, we offered a reward of 6 RMB to each respondent who submitted a valid response. We also included multiple screening questions to ensure that the respondents were indeed Alipay users. For example, at the beginning of the questionnaire, we asked the participants whether they had ever used mobile payment and whether they had ever used Alipay Wallet. If the response to either of these two questions was "never used", the questionnaire was automatically deemed invalid. The qualified respondents were required to answer the questions by recalling information pertaining to their experiences with using Alipay. By using the recall method, respondents are able to efficiently retrieve knowledge from memory, which helps them establish their current beliefs and actions [43]. In total, nearly 614 questionnaires were distributed, and 559 usable responses were collected. The response rate is 91%. Among the respondents (n = 559), 63% were female, 91.2% were below the age of forty, 75.4% held a bachelor's degree, 63.3% had a monthly income of 5000 RMB or above, and 83.8% reported having more than three years of experience using Alipay Wallet.

We assessed nonresponse bias by comparing the demographics and principal variables between the early 25% and late 25% of respondents. No significant differences in the principal variables were found, indicating that nonresponse bias was not a major concern. To address common method bias (CMB), we employed three tests for evaluation. First, Harman's single-factor test was conducted [44]. The results showed that the first factor accounted for only 36.5% of the variance, indicating that no single factor dominated the variance. It is preliminarily judged that CMB may not be severe. Second, we incorporated fashion consciousness as a marker variable in the survey [45]. The results indicate that, after the addition of the marker variable, the correlations among the variables remained unaltered, and the correlation between the marker variable and the other variables in the model was notably weaker than the correlations among the variables within the model (refer to Table S5 in the Supplementary Material). Third, we employed the unmeasured latent method construct (ULMC) to evaluate the CMB [46]. Model 1 serves as the baseline model, whereas Model 2 represents the model after the addition of the method factor. By comparing several crucial indicators of Model 1 and Model 2 ($RMR_{Model1} = 0.048$, $RMR_{Model2} = 0.049$; $RMSEA_{Model1} = 0.044$, $RMSEA_{Model2} = 0.044$; $NFI_{Model1} = 0.923$, $NFI_{Model2} = 0.923$, $CFI_{Model1} = 0.958$, $CFI_{Model2} = 0.958$; $\chi^2/df_{Model1} = 623.799/303 = 2.058$, $\chi^2/df_{Model2} = 621.904/302 = 2.059$), we found that there was no significant difference between these two models. All these findings demonstrate that there are no significant CMB issues in the present research. Additionally, we tested the VIFs of all items in the research model, and the results showed that all VIFs were less than 4 (see Table 1), indicating stable model estimation.

Table 1. Descriptive statistics of constructs.

Construct	Item	Loading	Mean	VIF
General structural assurance (GSA) AVE = 0.64; CR = 0.88; CA = 0.81	GSA 1	0.82	5.86	1.80
	GSA 2	0.78	5.74	1.53
	GSA 3	0.80	5.86	1.69
	GSA 4	0.80	5.87	1.72
General institutional structure (GIS) AVE = 0.57; CR = 0.84; CA = 0.75	GIS 1	0.78	5.43	1.53
	GIS 2	0.81	5.31	1.53
	GIS 3	0.77	5.06	1.50
	GIS 4	0.65	5.61	1.23
Local structural assurance (LSA) AVE = 0.62; CR = 0.87; CA = 0.80	LSA 1	0.82	5.81	1.68
	LSA 2	0.79	5.80	1.62
	LSA 3	0.77	5.74	1.52
	LSA 4	0.77	5.91	1.61
Local institutional structure (LIS) AVE = 0.63; CR = 0.87; CA = 0.80	LIS 1	0.71	5.24	1.43
	LIS 2	0.80	5.17	1.54
	LIS 3	0.81	5.21	1.88
	LIS 4	0.84	5.26	1.99
Trust (TRU) AVE = 0.63; CR = 0.87; CA = 0.81	TRU 1	0.82	5.68	1.72
	TRU 2	0.73	5.61	1.45
	TRU 3	0.81	5.31	1.7
	TRU 4	0.81	5.53	1.75
Privacy concern (PC) AVE = 0.80; CR = 0.94; CA = 0.92	PC 1	0.86	4.46	2.24
	PC 2	0.92	4.20	3.88
	PC 3	0.91	4.13	3.47
	PC 4	0.89	4.43	2.98
Self-disclosure (SD) AVE = 0.79; CR = 0.92; CA = 0.87	SD 1	0.89	4.90	2.15
	SD 2	0.89	5.15	2.27
	SD 3	0.89	5.14	2.28

Note: average extracted variance (AVE); composite reliability (CR); Cronbach's alpha (CA); variance inflation factor (VIF).

4.3. Measurement Development

We adopted previously validated scales to measure our constructs (refer to Table S4 in Supplementary Material). The scales for general institutional structure, general structure assurance, local institutional structure, and local structure assurance were adapted from Gong et al. [11]. The scales for trust and privacy concern were adapted from Sutanto et al. [47] and the scales for self-disclosure were adapted from Anderson & Agarwal [48]. We also controlled the impacts of consumer demographics (i.e., age, gender, education, income), usage experience, and usage frequency. The scales for information sensitivity were adapted from Dinev et al. [49]. We used a 7-point Likert scale (ranging from 1 = strongly disagree to 7 = strongly agree) to measure all of the constructs.

5. Data Analysis and Results

We used partial least squares (PLS) to empirically validate the research model and hypotheses. PLS is a component-based structural equation modeling technique that employed latent variables to assess path analytic modeling. Compared with covariance-based structural equation modeling (e.g., LISREL), PLS is more suitable for our prediction-oriented model as it tries to maximize the explained variance of endogenous variables [50]. We tested the measurement model and structural model using Smart PLS 3.0 with the standard bootstrapping of 5000 resamples [51].

5.1. Measurement Model

We validated the measurement model with three purposes: (1) to establish convergent validity; (2) to examine discriminant validity; and (3) to address concerns regarding multicollinearity [51]. Tables 1–3 present the PLS results of the measurement model. For convergent validity, we estimated the average extracted variance (AVE > 0.5), composite reliability (CR > 0.7), Cronbach's alpha (CA > 0.7), and item loadings (loadings > 0.7) of all constructs. For discriminant validity, we checked whether intra-construct correlations were smaller than the square root of the AVE of their respective constructs. For multicollinearity, we examined variance inflation factor values (VIFs < 5.0). The results indicate that our scales had acceptable convergent validity and discriminant validity, as well as minimal concern for multicollinearity.

Table 2. Item loadings and cross-loadings analysis.

Construct	Item	GSA	GIS	LSA	LIS	TRU	PC	SD
General institutional structure (GIS)	GSA 1	**0.82**	0.46	0.53	0.31	0.46	−0.20	0.29
	GSA 2	**0.78**	0.52	0.57	0.34	0.47	−0.23	0.28
	GSA 3	**0.80**	0.47	0.52	0.32	0.44	−0.27	0.30
	GSA 4	**0.80**	0.46	0.58	0.31	0.44	−0.18	0.25
General structural assurance (GSA)	GIS 1	0.50	**0.78**	0.47	0.45	0.49	−0.24	0.34
	GIS 2	0.54	**0.81**	0.51	0.50	0.56	−0.29	0.37
	GIS 3	0.40	**0.77**	0.35	0.53	0.46	−0.27	0.31
	GIS 4	0.35	**0.65**	0.43	0.39	0.43	−0.20	0.27
Local institutional structure (LIS)	LSA 1	0.60	0.50	**0.82**	0.44	0.57	−0.27	0.36
	LSA 2	0.53	0.46	**0.79**	0.38	0.54	−0.24	0.26
	LSA 3	0.53	0.48	**0.77**	0.39	0.50	−0.31	0.27
	LSA 4	0.50	0.40	**0.77**	0.34	0.48	−0.22	0.28
Local structure assurance (LSA)	LIS 1	0.28	0.45	0.35	**0.71**	0.46	−0.17	0.25
	LIS 2	0.33	0.54	0.41	**0.80**	0.61	−0.31	0.32
	LIS 3	0.30	0.48	0.38	**0.81**	0.54	−0.24	0.32
	LIS 4	0.35	0.50	0.42	**0.84**	0.57	−0.24	0.36
Trust (TRU)	TRU 1	0.51	0.53	0.60	0.58	**0.82**	−0.32	0.38
	TRU 2	0.46	0.46	0.53	0.44	**0.73**	−0.23	0.27
	TRU 3	0.41	0.53	0.48	0.60	**0.81**	−0.32	0.40
	TRU 4	0.42	0.53	0.49	0.58	**0.81**	−0.24	0.34
Privacy concern (PC)	PC 1	−0.22	−0.30	−0.26	−0.26	−0.31	**0.86**	−0.34
	PC 2	−0.26	−0.30	−0.30	−0.28	−0.31	**0.92**	−0.32
	PC 3	−0.26	−0.29	−0.32	−0.27	−0.32	**0.91**	−0.30
	PC 4	−0.24	−0.30	−0.29	−0.29	−0.32	**0.89**	−0.27
Self-disclosure (SD)	SD 1	0.33	0.42	0.34	0.40	0.42	−0.30	**0.89**
	SD 2	0.30	0.36	0.31	0.33	0.36	−0.33	**0.89**
	SD 3	0.30	0.36	0.33	0.32	0.38	−0.29	**0.89**

Note: bold diagonal represents the item loadings.

Table 3. Correlation matrix of the constructs.

	GSA	GIS	LSA	LIS	TRU	PC	SD
General structural assurance (GSA)	**0.80**						
General institutional structure (GIS)	0.59	**0.75**					
Local structural assurance (LSA)	0.68	0.57	**0.79**				
Local institutional structure (LIS)	0.40	0.62	0.49	**0.79**			
Trust (TRU)	0.57	0.64	0.66	0.69	**0.80**		
Privacy concern (PC)	−0.27	−0.33	−0.33	−0.30	−0.35	**0.90**	
Self-disclosure (SD)	0.35	0.43	0.37	0.39	0.44	−0.34	**0.89**

Note: bold diagonal represents the square root of AVEs.

5.2. Structural Model

The results of the measure model are shown in Figure 3 and Table 4, which indicate that H1, H2, H3, H5, H6, H7, H8, H9, and H10 were supported, while H4 was not. Overall, the R^2 values for trust, privacy concern, and self-disclosure behavior were 64%, 15%, and 27%, respectively. And we also test the indirect effect of trust and privacy concern (Table 5). Finally, the model had a good fit with an SRMR (standardized root mean square residual) value of 0.054, which compared the difference between the observed correlation and the predicted correlation as an adjustment measurement for the model, with the accepted value of lower than 0.08 [52].

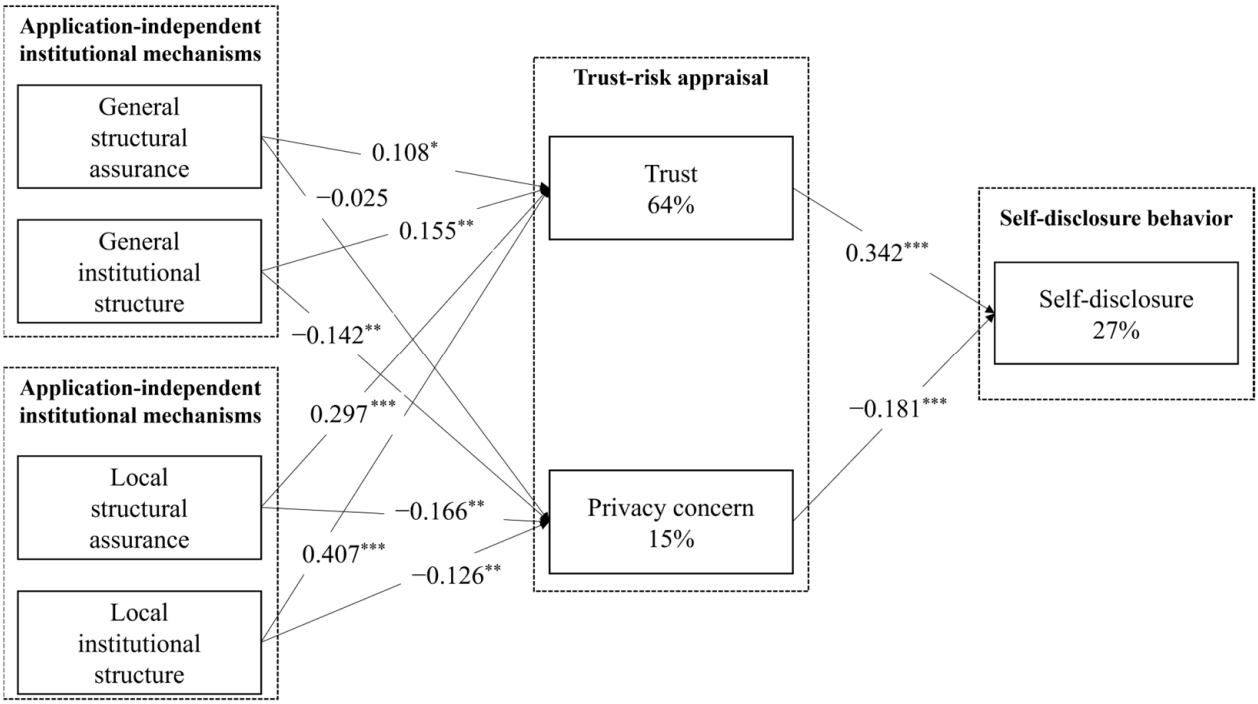


Figure 3. Structural model. *: $p < 0.05$; **: $p < 0.01$; ***: $p < 0.001$.

Table 4. Result of the structural model.

	β	*p*	95% CI
General structural assurance → Trust	0.108	0.044	[0.011, 0.221]
General structural assurance → Privacy concern	−0.025	0.578	[−0.116, 0.063]
General institutional structure → Trust	0.155	0.001	[0.068, 0.247]
General institutional structure → Privacy concern	−0.142	0.007	[−0.244, −0.037]
Local structural assurance → Trust	0.297	<0.001	[0.180, 0.410]
Local structural assurance → Privacy concern	−0.166	0.001	[−0.263, −0.070]
Local institutional structure → Trust	0.407	<0.001	[0.336, 0.476]
Local institutional structure → Privacy concern	−0.126	0.007	[−0.217, −0.032]
Trust → Self-disclosure	0.342	<0.001	[0.261, 0.419]
Privacy concern → Self-disclosure	−0.181	<0.001	[−0.258, −0.107]

Table 5. Result of the mediating effects.

		β	*p*	95% CI	Proportion of Mediation
Total effect	General structural assurance → Self-disclosure	0.042	0.051	[0.004, 0.089]	100%
Indirect effect	General structural assurance → Trust → Self-disclosure	0.037	0.054	[0.004, 0.081]	88%
	General structural assurance → Privacy concern → Self-disclosure	0.005	0.583	[−0.011, 0.023]	Non-significant
Total effect	General institutional structure → Self-disclosure	0.079	<0.001	[0.042, 0.121]	100%
Indirect effect	General institutional structure → Trust → Self-disclosure	0.053	0.002	[0.023, 0.091]	67%
	General institutional structure → Privacy concern → Self-disclosure	0.026	0.033	[0.006, 0.054]	33%
Total effect	Local structural assurance → Self-disclosure	0.132	<0.001	[0.086, 0.182]	100%
Indirect effect	Local structural assurance → Trust → Self-disclosure	0.102	<0.001	[0.059, 0.151]	77%
	Local structural assurance → Privacy concern → Self-disclosure	0.030	0.008	[0.012, 0.056]	23%
Total effect	Local institutional structure → Self-disclosure	0.162	<0.001	[0.123, 0.205]	100%
Indirect effect	Local institutional structure → Trust → Self-disclosure	0.139	<0.001	[0.103, 0.181]	86%
	Local institutional structure → Privacy concern → Self-disclosure	0.023	0.022	[0.006, 0.045]	14%

6. Discussion and Conclusions

The present study investigates the impact of institutional mechanisms on users' self-disclosure in mobile payment apps. Our research findings demonstrate that trust and privacy concerns play crucial roles in determining users' self-disclosure behavior within mobile payment apps. These results align with previous research on self-disclosure, which has consistently identified trust as a primary motivator for users to disclose personal information, while privacy concerns act as a significant deterrent. Our empirical findings also demonstrate the effective role of institutional mechanisms in promoting users' self-disclosure within mobile payment apps. Specifically, general institutional structure, local structural assurance, and local institutional structure positively influence trust levels while simultaneously reducing privacy concerns. Conversely, general structural assurance does not have a significant impact on privacy concerns and has a minor but significant impact on trust. This is in accordance with prospect theory [53], which indicates that users' aversion to potential losses is significantly stronger than their pursuit of gains. General structural assurance presents a "guaranteed success" gain-oriented framework, whereas general institutional structure directly tackles users' apprehensions regarding "what if it fails". It effectively manages their loss expectations by offering clear risk-mitigation and compensation mechanisms. Owing to the characteristic of loss aversion, general institutional structure, which directly addresses the consequences, exerts a greater influence than general structural assurance.

Moreover, it is noteworthy that local structural assurance and local institutional structure play a more significant role than general structural assurance and general institutional structure in fostering trust and mitigating privacy concerns. According to the construal level theory, general institutional mechanisms are characterized by a high psychological distance from users, manifesting as abstraction, remoteness, and non-specificity [54]. Although users are aware of such mechanisms and acknowledge their potential to safeguard

privacy, it remains difficult for them to directly perceive the real-time operational processes involved. As a result, these mechanisms primarily offer a background sense of security. When users encounter problems such as privacy leakage or fund theft, general institutional mechanisms, such as legal rights protection processes, are generally regarded as costly, lengthy, and having uncertain outcomes, and are thus perceived as inefficient by users. In contrast, local institutional mechanisms maintain a lower psychological distance, marked by concreteness, proximity, and interactivity. Users can directly perceive their presence through visual cues and operational interactions in real-time scenarios such as making payments or granting authorizations. This accessible form of security exerts a more substantial impact on users' decision making.

These findings suggest that, in a highly mature and fiercely competitive market such as mobile payment, robust security technologies (e.g., general structural assurance) are no longer a significant advantage but merely a basic expectation of users. When all countries and industries have established high-level structural safeguards, these safeguards no longer hold significant signaling value. Users take it for granted that all general structural assurance should be universally implemented. Secondly, as users become increasingly familiar with digital services, they develop an inherent trust in the macro-environment, believing that the entire system is regulated. Therefore, their cognitive resources and attention are no longer focused on the macro-level question of whether the industry is safe, but rather on the specific platforms directly related to their current operations. The questions they are more concerned about are: What specific technologies does the app I'm currently using have to protect me? If my information is leaked on this app, how will it be held accountable to me? This shift in attention also makes the local institutional mechanisms of those specific platforms more prominent and crucial.

6.1. Theoretical Implications

The present study has several theoretical implications. First, our research contributes to the existing self-disclosure literature by identifying the impact of institutional mechanisms on users' self-disclosure behavior. While previous studies have proposed various factors that influence self-disclosure in online environments, most of these factors primarily focus on sociopsychological aspects such as trust, privacy concerns, benefits and risks associated with privacy, emotions, affective commitment, and perceived invasion. However, the significance of institutional mechanisms in influencing self-disclosure has received little attention. Our study addresses this knowledge gap by examining the effectiveness of institutional mechanisms in facilitating self-disclosure within mobile payment apps through trust-building strategies and reducing privacy concerns. This complementary perspective enhances our comprehension of the factors influencing self-disclosure in online environments. Moreover, the present study demonstrates that there exist substantial hierarchical effects and context dependencies in the influence of institutional mechanisms on trust and privacy concerns. The results suggest that, in the mobile payment environment, the impact of institutional mechanisms is different. By differentiating between general institutional mechanisms and local institutional mechanisms in the mobile payment context and empirically validating that the latter exerts a greater influence on user trust and privacy concerns than the former, this study emphasizes that in specific contexts (such as high-frequency interaction digital platforms), local institutional mechanisms that directly interact with individuals and offer immediate feedback are the crucial drivers in shaping behavior and cognition. Consequently, future institutional mechanisms research, particularly in areas related to individual decision making, should pay greater attention to the more specific and direct local institutional mechanisms within the specific context.

Secondly, the present work contributes to the mobile payment literature by stressing the value of users' self-disclosure. Previous studies on users' adoption and usage of mobile payment apps have predominantly relied on general technology adoption models [55,56]. However, limited research has specifically investigated users' self-disclosure in mobile payment apps. One possible explanation is that mobile payment apps are still considered developing financial technologies, making user adoption and usage behavior a crucial concern for most mobile payment providers. Given that mobile payment apps need to cater to various payment scenarios such as peer-to-peer money transfers, credit card repayments, and supermarket checkouts, the collection and utilization of personal information becomes an inevitable aspect of delivering accurate and personalized financial services through these platforms. Our study intends to bridge this knowledge gap by investigating self-disclosure in mobile payment apps, thereby serving as a starting point for future research in this field. Finally, our work extends the two-dimensional topology of institutional mechanisms from the traditional e-commerce environment to the emerging mobile payment industry and empirically examines the impact of institutional mechanisms on users' self-disclosure in mobile payment apps.

6.2. Practical Implications

The conclusions of this study have substantial practical consequences for the mobile payment industry. It is crucial to prioritize the facilitation of users' self-disclosure for mobile payment providers and stakeholders. While the acquisition and utilization of personal information are inherent aspects in the mobile payment industry, consumers are unlikely to willingly disclose their personal information unless they possess a high level of trust and minimal privacy concerns. To encourage users' self-disclosure, it is imperative for mobile payment providers and stakeholders to devise strategies that foster user trust and alleviate apprehensions regarding information privacy. Our empirical results demonstrate that establishing institutional mechanisms effectively promotes users' self-disclosure in mobile payment apps.

First, prioritize strategic investment in local institutional structure. Given that local institutional structure has the most significant impact on enhancing trust, platforms should make it the core of resource allocation. For example, direct financial guarantee commitments, such as Alipay's "Account Security Insurance", are beneficial initiatives. We further propose that platforms not only provide such guarantees but also remove them from their hidden placement within long-winded user agreements. Platforms should highlight these guarantees during crucial decision-making moments, such as payment and transfer, via active push notifications and prominent markings. Although this approach entails higher financial and human resource costs, its leveraging effect on trust building justifies the investment. Second, focus on enhancing local structural assurance. The findings show that local structural assurance is the most effective in alleviating users' privacy concerns. Therefore, platforms should allocate resources to technological and design innovations that enhance users' perceived security. Alipay's "Privacy Settings Center" is a positive step, but there is still room for improvement. Specific improvement directions include using layered pop-ups, short videos, and other visual means to explain data usage, and providing more detailed and user-friendly privacy control options.

Finally, it is recommended that stakeholders within the mobile payment industry, including regulatory associations and government agencies, establish effective, application-independent institutional mechanisms: general structural assurance and a general institutional structure. The findings indicate that although general structural assurance has a weak yet statistically significant positive influence on trust, it is ineffective in mitigating privacy concerns. This does not imply that general structural assurance is unimportant.

Rather, users perceive it as a fundamental guarantee of the industry. It suggests that, in the mobile payment domain, general structural assurance primarily functions as an endorser of industry legitimacy rather than a core driver of trust. Moreover, this research demonstrates that the general institutional structure has a substantial impact on enhancing user trust and alleviating privacy concerns. Therefore, the responsibility of regulators should be centered on enhancing the transparency of top-level institutional design and enforcement. For example, promoting the transformation of platform compensation commitments from voluntary actions into legally regulated mandatory obligations, establishing industry joint compensation funds and standardized dispute resolution mechanisms, and improving post-event accountability systems. Additionally, promoting legislation regarding data governance transparency is essential. Data protection should be established as a legal standard for all digital applications, ensuring that users can conveniently exercise their data rights through a unified and clear interface.

6.3. Limitations and Future Research

This study has some limitations and therefore offers opportunities for future research. First, our work invited users of a well-known mobile payment app (Alipay Wallet) in China to examine our research model. Future investigations should include various mobile payment apps, such as WeChat Wallet, Apple Pay, PayPal, and Samsung Pay, in order to assess the generalizability of the current model. Specifically, the popular mobile payment applications vary across different countries. Therefore, by including various mobile payment applications, we can explore the different impacts of general institutional mechanisms on self-disclosure in different national contexts.

Second, our work shows that institutional mechanisms are important in fostering trust and alleviating privacy concerns in the formation of users' self-disclosure. The boundary conditions underlying how institutional mechanisms affect trust and privacy concerns should be the focus of future research. For example, two promising areas are the interplay between platform and country characteristics and the role of algorithm transparency. These boundary conditions may offer a deeper understanding of the circumstances under which application-specific institutional mechanisms are more effective and those under which application-independent institutional mechanisms are more important in building trust and alleviating privacy concerns.

Third, the current research utilizes a cross-sectional, self-reported survey design. The temporal stability and causal directions of the observed associations remain uncertain. Future studies could adopt a longitudinal design to capture the dynamic process through which institutional mechanisms exert influence. Scenario experiments serve as an effective tool for rigorously testing causal relationships. Researchers can design various application interfaces to present to subjects in order to manipulate local and general institutional mechanisms. Furthermore, integrating objective behavioral data would help reduce reliance on self-reporting and provide a more comprehensive understanding.

Finally, the results show that the proportion of respondents under 40 years old reaches 91.2%, mainly due to two reasons. First, as an online payment application, the usage rate of Alipay Wallet among people over 60 years old is relatively low. Second, this questionnaire was distributed online, limiting its reach to older individuals. Furthermore, our data indicate that age has a significantly negative impact on privacy concerns yet has no significant effect on trust. This directly contradicts the common belief that older individuals should be more worried about privacy leaks. A plausible explanation is that young people have come of age in an era of information explosion and possess a profound understanding of how data is collected, utilized, and misused, along with the associated consequences. Conversely, older users, owing to their inadequate understanding

of privacy leaks in the digital age, underestimate the potential privacy risks. Future research could employ alternative methods to address the data bias caused by demographic imbalances. For instance, it could incorporate offline interviews to increase the sample size of the elderly, thereby more accurately capturing the differences in privacy perception between generations.

6.4. Conclusions

The collection and use of personal information are an unavoidable element of mobile payment. However, there is substantial evidence that users are hesitant to share their personal information with mobile payment apps due to privacy and security concerns. In this study, we develop a research model to understand users' self-disclosure in mobile payment apps and highlight the effect of institutional mechanisms. Our empirical findings show that institutional mechanisms are effective in building users' trust and alleviating privacy concerns, which ultimately facilitate their self-disclosure in mobile payment apps.

Supplementary Materials: The following supporting information can be downloaded at: https://www.mdpi.com/article/10.3390/jtaer21010010/s1, Table S1: Literature Review on Mobile Payment; Table S2: Literature Review on Self-Disclosure; Table S3: Literature Review on Institutional Mechanisms; Table S4: Constructs and Measurements; Table S5: Correlation Marker Technique.

Author Contributions: Conceptualization, H.X. and J.L.; methodology, H.X.; validation, J.L.; formal analysis, H.X.; investigation, H.X.; resources, J.L.; data curation, H.X.; writing—original draft preparation, H.X.; writing—review and editing, J.L.; visualization, H.X.; supervision, J.L.; project administration, J.L.; funding acquisition, J.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Key Project of the Anhui Provincial Department of Education, grant number 2024AH052216, and the project of Anhui Province Natural Science Foundation of China, grant number 2408085QG226.

Institutional Review Board Statement: This research was carried out via an online questionnaire survey, ensuring complete anonymity for participants. In accordance with the "Notice on the Issuance of the Measures for Ethical Review of Life Science and Medical Research Involving Human Beings" jointly published by the National Health Commission, the Ministry of Education, the Ministry of Science and Technology, and the National Administration of Traditional Chinese Medicine, research utilizing anonymized information data is exempt from ethical review to alleviate unnecessary burdens on researchers (Article.32).

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors upon reasonable request.

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

References

1. An, S.; Cheung, C.F.; Willoughby, K.W. A Gamification Approach for Enhancing Older Adults' Technology Adoption and Knowledge Transfer: A Case Study in Mobile Payments Technology. *Technol. Forecast. Soc. Change* **2024**, *205*, 123456. [CrossRef]
2. Hew, J.-J.; Lee, V.-H.; Leong, L.-Y. Deciphering the Resistance Behaviours towards Mobile Commerce Applications: A Mobile Commerce Applications Resistance Theory (MOCART). *Comput. Hum. Behav.* **2024**, *151*, 108033. [CrossRef]
3. Chen, R.; Zolbanin, H.M.; Gentina, E. Pseudo-Community Trust and Member Self-Disclosure: An Empirical Study. *Inf. Manag.* **2024**, *61*, 104001. [CrossRef]
4. Wu, D.; Min, C.; Li, Z.; Wang, Y. Vigilance and Habituation: Polymorphic Experience Effects in Internet Users' Privacy Disclosure Decisions. *Decis. Support Syst.* **2023**, *170*, 113961. [CrossRef]
5. Zhang, J.; Wang, W.; Khansa, L.; Kim, S. Actual Private Information Disclosure on Online Social Networking Sites: A Reflective-Impulsive Model. *JAIS* **2024**, *25*, 1533–1562. [CrossRef]

6. Chauhan, V. Understanding Users' Protective Behavior and Its Suppressor Effect on the Perceived Risk in M-Wallet/Banking Use: An Indian Urban-Rural Comparison. *Technol. Forecast. Soc. Change* **2024**, *201*, 123255. [CrossRef]
7. Alashoor, T.; Keil, M.; Smith, H.J.; McConnell, A.R. Too Tired and in Too Good of a Mood to Worry About Privacy: Explaining the Privacy Paradox Through the Lens of Effort Level in Information Processing. *Inf. Syst. Res.* **2023**, *34*, 1415–1436. [CrossRef]
8. Krasnova, H.; Spiekermann, S.; Koroleva, K.; Hildebrand, T. Online Social Networks: Why We Disclose. *J. Inf. Technol.* **2010**, *25*, 109–125. [CrossRef]
9. Zhang, S.; Huang, F.; Yu, L.; Wang, J.F.; Lowry, P.B. A Dual-Process Model to Explain Self-Disclosure on Online Social Networking Sites: Examining the Moderating Effect of Enjoyment. *INTR* **2024**, *34*, 1456–1487. [CrossRef]
10. Vaghefi, M.S.; Nazareth, D.L.; Nerur, S.P.; Chen, K.-Y. Self-Disclosure in Online Social Networks: An Empirical Study of Location-Based Check-Ins and Impression Management. *Inf. Manag.* **2024**, *61*, 104017. [CrossRef]
11. Gong, X.; Cheung, C.M.K.; Liu, S.; Zhang, K.Z.K.; Lee, M.K.O. Battles of Mobile Payment Networks: The Impacts of Network Structures, Technology Complementarities and Institutional Mechanisms on Consumer Loyalty. *Inf. Syst. J.* **2022**, *32*, 696–728. [CrossRef]
12. Gong, X.; Zhang, K.Z.K.; Chen, C.; Cheung, C.M.K.; Lee, M.K.O. What Drives Trust Transfer from Web to Mobile Payment Services? The Dual Effects of Perceived Entitativity. *Inf. Manag.* **2020**, *57*, 103250. [CrossRef]
13. Johnson, V.L.; Kiser, A.; Washington, R.; Torres, R. Limitations to the Rapid Adoption of M-Payment Services: Understanding the Impact of Privacy Risk on M-Payment Services. *Comput. Hum. Behav.* **2018**, *79*, 111–122. [CrossRef]
14. Xu, Y.; Ghose, A.; Xiao, B. Mobile Payment Adoption: An Empirical Investigation of Alipay. *Inf. Syst. Res.* **2024**, *35*, 807–828. [CrossRef]
15. Al-Natour, S.; Benbasat, I.; Cenfetelli, R. Designing Online Virtual Advisors to Encourage Customer Self-Disclosure: A Theoretical Model and an Empirical Test. *J. Manag. Inf. Syst.* **2021**, *38*, 798–827. [CrossRef]
16. Sun, Y.; Wang, N.; Shen, X.-L. Calculus Interdependency, Personality Contingency, and Causal Asymmetry: Toward a Configurational Privacy Calculus Model of Information Disclosure. *Inf. Manag.* **2021**, *58*, 103556. [CrossRef]
17. Gong, X.; Zhang, K.Z.K.; Chen, C.; Cheung, C.M.K.; Lee, M.K.O. What Drives Self-Disclosure in Mobile Payment Applications? The Effect of Privacy Assurance Approaches, Network Externality, and Technology Complementarity. *ITP* **2019**, *33*, 1174–1213. [CrossRef]
18. Kordzadeh, N.; Warren, J. Communicating Personal Health Information in Virtual Health Communities: An Integration of Privacy Calculus Model and Affective Commitment. *JAIS* **2017**, *18*, 45–81. [CrossRef]
19. Bansal, G.; "Mariam" Zahedi, F.; Gefen, D. The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in Disclosing Health Information Online. *Decis. Support Syst.* **2010**, *49*, 138–150. [CrossRef]
20. Jiang, Z.; Heng, C.S.; Choi, B.C.F. Research Note—Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions. *Inf. Syst. Res.* **2013**, *24*, 579–595. [CrossRef]
21. Wang, J.; Dong, M.; Yang, Z.; Li, Y. Passing the Torch: How Parental Privacy Concerns Affect Adolescent Self-Disclosure on Social Networking Sites. *MIS Q.* **2023**, *47*, 1585–1614. [CrossRef]
22. Yan, R.; Gong, X.; Xu, H.; Yang, Q. Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Online Self-Disclosure. *INTR* **2024**. [CrossRef]
23. Bansal, G.; Mariam Zahedi, F.; Gefen, D. The Role of Privacy Assurance Mechanisms in Building Trust and the Moderating Role of Privacy Concern. *Eur. J. Inf. Syst.* **2015**, *24*, 624–644. [CrossRef]
24. Pavlou, P.A.; Gefen, D. Building Effective Online Marketplaces with Institution-Based Trust. *Inf. Syst. Res.* **2004**, *15*, 37–59. [CrossRef]
25. Fang, Y.; Qureshi, I.; Sun, H.; McCole, P.; Ramsey, E.; Lim, K.H. Trust, Satisfaction, and Online Repurchase Intention: The Moderating Role of Perceived Effectiveness of E-Commerce Institutional Mechanisms. *MIS Q.* **2014**, *38*, 407–427. [CrossRef]
26. Zhou, T. Understanding Users' Initial Trust in Mobile Banking: An Elaboration Likelihood Perspective. *Comput. Hum. Behav.* **2012**, *28*, 1518–1525. [CrossRef]
27. Gefen, D.; Pavlou, P.A. The Boundaries of Trust and Risk: The Quadratic Moderating Role of Institutional Structures. *Inf. Syst. Res.* **2012**, *23*, 940–959. [CrossRef]
28. Montazemi, A.R.; Qahri-Saremi, H. Factors Affecting Adoption of Online Banking: A Meta-Analytic Structural Equation Modeling Study. *Inf. Manag.* **2015**, *52*, 210–226. [CrossRef]
29. Luo, X.; Li, H.; Zhang, J.; Shim, J.P. Examining Multi-Dimensional Trust and Multi-Faceted Risk in Initial Acceptance of Emerging Technologies: An Empirical Study of Mobile Banking Services. *Decis. Support Syst.* **2010**, *49*, 222–234. [CrossRef]
30. Gefen, D.; Karahanna, E.; Straub, D.W. Trust and TAM in Online Shopping: An Integrated Model. *MIS Q.* **2003**, *27*, 51–90. [CrossRef]
31. Konuk, F.A. The Influence of Perceived Food Quality, Price Fairness, Perceived Value and Satisfaction on Customers' Revisit and Word-of-Mouth Intentions towards Organic Food Restaurants. *J. Retail. Consum. Serv.* **2019**, *50*, 103–110. [CrossRef]

32. Yang, K.; Kim, H.M.; Tanoff, L. Signaling Trust: Cues from Instagram Posts. *Electron. Commer. Res. Appl.* **2020**, *43*, 100998. [CrossRef]
33. Liu, H.; Chou, H. The Impact of Regulatory Focus on the Inaction Inertia Effect. *Psychol. Mark.* **2025**, *42*, 1779–1794. [CrossRef]
34. Wakefield, R. The Influence of User Affect in Online Information Disclosure. *J. Strateg. Inf. Syst.* **2013**, *22*, 157–174. [CrossRef]
35. Cichy, P.; Salge, T.O.; Kohli, R. Privacy Concerns and Data Sharing in the Internet of Things: Mixed Methods Evidence from Connected Cars. *MISQ* **2021**, *45*, 1863–1892. [CrossRef]
36. Shao, Z.; Zhang, L.; Brown, S.A.; Zhao, T. Understanding Users' Trust Transfer Mechanism in a Blockchain-Enabled Platform: A Mixed Methods Study. *Decis. Support Syst.* **2022**, *155*, 113716. [CrossRef]
37. Sha, W. Types of Structural Assurance and Their Relationships with Trusting Intentions in Business-to-Consumer e-Commerce. *Electron Mark.* **2009**, *19*, 43–54. [CrossRef]
38. Dahlberg, T.; Guo, J.; Ondrus, J. A Critical Review of Mobile Payment Research. *Electron. Commer. Res. Appl.* **2015**, *14*, 265–284. [CrossRef]
39. Mousavizadeh, M.; Kim, D.J.; Chen, R. Effects of Assurance Mechanisms and Consumer Concerns on Online Purchase Decisions: An Empirical Study. *Decis. Support Syst.* **2016**, *92*, 79–90. [CrossRef]
40. Srivastava, S.C.; Chandra, S. Social Presence in Virtual World Collaboration: An Uncertainty Reduction Perspective Using a Mixed Methods Approach. *MIS Q.* **2018**, *42*, 779–803. [CrossRef]
41. Pan, Y.; Wan, Y.; Fan, J.; Liu, B.; Archer, N. Raising the Cohesion and Vitality of Online Communities by Reducing Privacy Concerns. *Int. J. Electron. Commer.* **2017**, *21*, 151–183. [CrossRef]
42. Oliveira, T.; Faria, M.; Thomas, M.A.; Popovič, A. Extending the Understanding of Mobile Banking Adoption: When UTAUT Meets TTF and ITM. *Int. J. Inf. Manag.* **2014**, *34*, 689–703. [CrossRef]
43. Kim, S.S. The Integrative Framework of Technology Use: An Extension and Test. *MIS Q.* **2009**, *33*, 513. [CrossRef]
44. Podsakoff, P.M.; MacKenzie, S.B.; Lee, J.-Y.; Podsakoff, N.P. Common Method Biases in Behavioral Research A Critical Review of the Literature and Recommended Remedies. *J. Appl. Psychol.* **2003**, *88*, 879–903. [CrossRef]
45. Malhotra, N.K.; Kim, S.S.; Patil, A. Common Method Variance in IS Research: A Comparison of Alternative Approaches and a Reanalysis of Past Research. *Manag. Sci.* **2006**, *52*, 1865–1883. [CrossRef]
46. Richardson, H.A.; Simmering, M.J.; Sturman, M.C. A Tale of Three Perspectives: Examining Post Hoc Statistical Techniques for Detection and Correction of Common Method Variance. *Organ. Res. Methods* **2009**, *12*, 762–800. [CrossRef]
47. Sutanto, J.; Palme, E.; Tan, C.-H.; Phang, C.W. Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users. *MIS Q.* **2013**, *37*, 1141–1164. [CrossRef]
48. Anderson, C.L.; Agarwal, R. The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information. *Inf. Syst. Res.* **2011**, *22*, 469–490. [CrossRef]
49. Dinev, T.; Xu, H.; Smith, J.H.; Hart, P. Information Privacy and Correlates: An Empirical Attempt to Bridge and Distinguish Privacy-Related Concepts. *Eur. J. Inf. Syst.* **2013**, *22*, 295–316. [CrossRef]
50. 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]
51. Hair, J.F.; Hult, G.T.M.; Ringle, C.; Sarstedt, M. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*; Sage Publications: Thousand Oaks, CA, USA, 2016; ISBN 978-4522-1744-4.
52. Henseler, J.; Ringle, C.M.; Sarstedt, M. A New Criterion for Assessing Discriminant Validity in Variance-Based Structural Equation Modeling. *J. Acad. Mark. Sci.* **2015**, *43*, 115–135. [CrossRef]
53. Tversky, A.; Kahneman, D. Loss Aversion in Riskless Choice: A Reference-Dependent Model. *Q. J. Econ.* **1991**, *106*, 1039–1061. [CrossRef]
54. Williams, L.E.; Stein, R.; Galguera, L. The Distinct Affective Consequences of Psychological Distance and Construal Level. *J. Consum. Res.* **2014**, *40*, 1123–1138. [CrossRef]
55. Liébana-Cabanillas, F.; Kalinic, Z.; Muñoz-Leiva, F.; Higueras-Castillo, E. Biometric M-Payment Systems: A Multi-Analytical Approach to Determining Use Intention. *Inf. Manag.* **2024**, *61*, 103907. [CrossRef]
56. Mishra, V.; Walsh, I.; Srivastava, A. Merchants' Adoption of Mobile Payment in Emerging Economies: The Case of Unorganised Retailers in India. *Eur. J. Inf. Syst.* **2022**, *31*, 74–90. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.