INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES
Vol 16, Issue 4, (2026) E-ISSN: 2222-6990

Understanding Continuance Intention toward Facial Recognition Payment: An Integration of ECM and APCO Frameworks

Zhu Fei
School of Management, Universiti Sains Malaysia, Penang, Malaysia
Email: zhufei2024@student.usm.my

Normalini Md Kassim*
School of Management, Sains Malaysia, Penang, Malaysia
*Corresponding Author Email: normalini@usm.my

DOI Link: http://dx.doi.org/10.6007/IJARBSS/v16-i4/28050

Published Date: 09 April 2026

Abstract
This study investigates the factors influencing Chinese users' continuance intention toward facial recognition payment (FRP) by integrating the Expectation Confirmation Model (ECM) and the Antecedents–Privacy Concerns–Outcomes (APCO) framework. A quantitative research design was adopted, and data were collected from 369 valid respondents using an online survey. Partial Least Squares Structural Equation Modeling (PLS-SEM) was employed to test the proposed hypotheses. The results indicate that satisfaction is the strongest predictor of continuance intention, followed by privacy concerns, which exert a significant but weaker negative effect. Expectation confirmation significantly influences both perceived usefulness and satisfaction, while perceived usefulness further enhances satisfaction. Privacy experience increases privacy concerns, whereas privacy awareness unexpectedly reduces them. In addition, privacy concerns negatively affect both satisfaction and continuance intention. The findings reveal that users do not simply ignore privacy risks; rather, they engage in a trade-off process in which perceived benefits outweigh perceived risks. This study contributes to the literature by integrating ECM and APCO to explain post-adoption behavior and by providing empirical evidence of the privacy paradox in the context of facial recognition payment. Practical implications are offered for service providers and policymakers to balance technological convenience and privacy protection.

Keywords: Facial Recognition Payment, Continuance Intention, Expectation Confirmation Model, Apco Framework, Privacy Concerns, Privacy Paradox

Introduction

In recent years, the rapid advancement of digital technologies, together with the increased demand for contactless services during the COVID-19 pandemic, has accelerated the global shift toward digital and cashless transactions (Kim et al., 2021). In response to these changes, FinTech providers have continuously promoted innovations in digital payment technologies, driving the transformation of payment systems from traditional cash- and card-based models to more intelligent and contactless forms (Al-Sharafi et al., 2022). Within this context, biometric payment technologies have rapidly emerged as a key component of digital payment systems (Dargan & Kumar, 2020). Compared with traditional authentication methods such as passwords, PIN codes, and physical bank cards, biometric payment relies on users' inherent physiological characteristics, which are less likely to be forgotten, lost, or easily replicated. As a result, it is generally considered to offer both higher security and greater convenience (Esteban & Daniel, 2016; Zhang & Kang, 2019).

Among various biometric payment methods, facial recognition payment (FRP) has attracted significant attention due to its non-invasive nature, relatively high accuracy, and low adoption barriers (Ricardo et al., 2016). Users can complete transactions simply by scanning their faces, without the need for mobile devices, bank cards, or additional hardware. Driven by these advantages, FRP has expanded rapidly worldwide, with China emerging as one of the most representative markets for its commercialization and everyday use (Liu et al., 2021). Supported by the rapid development of 5G, artificial intelligence, and mobile payment infrastructures, FRP has been widely integrated into various sectors in China, including retail, transportation, healthcare, hospitality, and online platforms (Li & Li, 2023). Currently, the Chinese FRP market is largely dominated by Tencent and Alibaba, and facial recognition payment has gradually become a routine payment method for many consumers (Limedia, 2019; Wang, 2024).

Despite its efficiency and convenience, the widespread adoption of FRP has raised increasing concerns regarding privacy and security risks (Hu et al., 2023). Biometric data are widely regarded as one of the most sensitive forms of personal information (Jones, 2020). Unlike passwords or PIN codes, facial data cannot be easily changed once compromised, making it difficult for users to mitigate potential damage (Li & Li, 2023). More importantly, facial information may not only lead to financial risks but also be used for surveillance, identity misuse, or other third-party purposes, thereby posing long-term threats to personal privacy, autonomy, and dignity (Yeung et al., 2020). In addition, due to the contactless and often invisible processes of data collection and processing, users may not be able to detect when their facial data are collected, shared, or misused, nor can they take timely remedial actions. This further amplifies the potential risks associated with FRP (Chen & Wang, 2023).

In the Chinese context, these issues are particularly salient. On the one hand, existing studies indicate that Chinese users are not indifferent to the risks of facial recognition technologies. Public debates, legal disputes, and social criticisms related to facial data collection and usage have become increasingly prominent (Cheng & Shao, 2019; Ding, 2019; Yan et al., 2020). Survey evidence also suggests that many users still prefer traditional authentication methods and even oppose the use of facial recognition in payment scenarios (Kostka et al., 2021; Liu et al., 2022). On the other hand, FRP continues to expand rapidly and is frequently used in everyday life, creating a notable paradox: users express relatively high privacy concerns and limited trust, yet continue to use this technology extensively. Compared with Western countries, Chinese users exhibit higher levels of actual adoption and continued usage of FRP despite comparable or even higher privacy concerns (Bromberg et al., 2020). Therefore, explaining why Chinese users continue to use FRP under high perceived privacy risks has become a critical research question.

This phenomenon also reflects the "Collingridge Dilemma"(Collingridge, 1982) in technological governance. That is, in the early stages of technological development, potential negative consequences are not sufficiently visible to justify strict regulation; however, once such consequences become apparent, the technology is often already deeply embedded in social systems, making regulation difficult and costly (Kudina & Verbeek, 2019). As FRP becomes increasingly institutionalized and normalized within China's payment ecosystem, its associated privacy risks are gradually evolving from latent concerns into tangible governance challenges. Therefore, examining why privacy concerns fail to inhibit the long-term use of FRP is crucial for understanding the diffusion logic of emerging payment technologies as well as for informing regulatory practices.

Although prior studies have explored the determinants of FRP usage, several limitations remain. First, information systems research distinguishes between initial adoption and post-adoption behavior. While initial acceptance explains why users begin to use a technology, continuance intention is more critical for ensuring the long-term success and sustainability of an information system (Bhattacherjee, 2001b; Rasul et al., 2023; Shahzad et al., 2024). However, existing FRP research has primarily focused on pre-adoption stages, examining users' intention to use or accept the technology (Hu et al., 2023; Hwang et al., 2024; Li et al., 2020; Lyu et al., 2024; Moriuchi, 2021), while paying limited attention to post-adoption behavior. Second, as FRP has entered a relatively mature stage in China, it is no longer sufficient to focus solely on pre-use expectations. It remains unclear whether users' expectations are confirmed after actual use, how post-consumption perceptions of usefulness are formed, and how these evaluations influence continuance intention. Third, although the privacy paradox has been widely discussed in the broader digital privacy literature, its underlying mechanism in the context of facial recognition payment (particularly in China) remains underexplored. While previous studies suggest that Chinese users may trade privacy for convenience (Kostka et al., 2021; Nemati et al., 2014), there is still a lack of an integrated framework that explains how privacy costs, perceived benefits, and continuance behavior interact.

To address these gaps, this study integrates the Antecedents–Privacy Concerns–Outcomes (APCO) model with the Expectation Confirmation Model (ECM) to develop an extended framework for examining Chinese users' continuance intention toward facial recognition payment. Specifically, this study investigates how privacy-related perceptions and post-adoption evaluations jointly influence continued usage, thereby providing a more comprehensive explanation of the coexistence of high privacy concerns and sustained usage in the Chinese FRP context. This study contributes to the literature in two main ways. Theoretically, it extends research on FRP by integrating privacy paradox perspectives with post-adoption behavior, offering a more comprehensive analytical framework for understanding user behavior in digital payment contexts. Practically, it provides empirical insights for the sustainable development, platform governance, and privacy regulation of facial recognition payment technologies, thereby addressing the broader challenges associated with the rapid expansion of emerging payment systems.

Literature Review

Expectancy Confirmation Model (ECM)

In the information systems (IS) literature, the Expectation Confirmation Model (ECM) proposed by Bhattacherjee (2001) is widely regarded as one of the most influential frameworks for explaining users' post-adoption behavior. It is considered a landmark model because it distinguishes between initial acceptance and continued usage, thereby extending the focus of IS research from adoption to long-term system use (Chiu et al., 2020; Lee & Kwon, 2011). While established models such as the Technology Acceptance Model (TAM) (Davis et al., 1989) and the Theory of Planned Behavior (TPB) (Ajzen, 1991) have been widely used to explain initial acceptance of new technologies, they are less effective in explaining users' behavior after adoption. However, the long-term success of an IS depends not only on initial acceptance but also on users' sustained engagement over time (Ambalov, 2018; Bhattacherjee, 2001a).

ECM was developed from Expectation Confirmation Theory (ECT), which was originally used to explain consumers' repurchase intention. Nevertheless, the direct application of ECT to the IS context is limited. First, expectation formation in IS settings is often more complex than in conventional consumer contexts. Because many technologies are novel, users may form expectations based on diverse sources, such as prior experience, attitudes, desire, and personal or commercial communication, and these expectations may vary considerably across individuals (Khalifa & Liu, 2004). Second, ECT mainly focuses on product performance and repurchase intention, which makes it less capable of capturing IS-specific dimensions such as system quality, information quality, and service quality. It therefore cannot fully explain user satisfaction in IS environments (Khalifa & Liu, 2004). In addition, ECT is rooted in a consumer context, whereas IS studies are more concerned with the "user" as the actual user of the system rather than merely the purchaser of a product or service.

To address these limitations, Bhattacherjee (2001) proposed ECM as a post-adoption model tailored to the IS context. Unlike ECT, ECM places greater emphasis on post-usage evaluations rather than pre-use expectations. It assumes that the effects of pre-adoption beliefs are already reflected in users' confirmation and satisfaction after actual system use. In this model, the traditional expectation construct is replaced by post-usage perceived usefulness, because users' beliefs about a system tend to evolve through experience. To distinguish it from TAM's pre-adoption perceived usefulness, later studies further described this construct as "post-usage usefulness," highlighting its experience-based and relatively stable nature (Bhattacherjee et al., 2008).

ECM also reconceptualizes several key elements of ECT for IS research. Repurchase intention is reformulated as continuance intention, and confirmation is defined as the degree to which users perceive congruence between their prior expectations and the system's actual performance (Bhattacherjee, 2001). The model further omits the explicit performance construct used in ECT, on the assumption that performance is already captured through confirmation. In this way, ECM provides a more parsimonious and context-appropriate explanation of continuance behavior in IS use.

According to ECM, continuance intention is determined by three core variables: confirmation, satisfaction, and post-usage perceived usefulness. After using a system for some time, users form an evaluation of its usefulness based on actual experience. They then compare this experience with their prior expectations and assess whether those expectations have been confirmed. A higher level of confirmation enhances user satisfaction and also strengthens post-usage perceived usefulness. Satisfaction subsequently promotes continuance intention, while perceived usefulness may also exert a direct effect on continuance intention because users are more likely to continue using a system when they perceive it to be beneficial to their needs (Bhattacherjee et al., 2008).

Given that this study examines the post-adoption behavior of facial recognition payment users in China, ECM provides a suitable theoretical foundation. In particular, it offers a useful lens for explaining how users evaluate whether their pre-adoption expectations have been confirmed through actual use, and how such evaluations shape satisfaction and continuance intention in a mature usage context.

Antecedent-Privacy Concern-Outcome (APCO) Macro Model

Privacy has long been a central construct in information systems research, yet it remains inherently difficult to quantify (Smith et al., 2011). As a result, prior studies have commonly operationalized privacy through the concept of privacy concerns, defined as individuals' perceived risk that their personal information may be misused when disclosed to external entities (Dinev & Hart, 2005; Xu et al., 2011). Privacy concerns play a crucial role in shaping users' trust in organizations and their strategies for managing personal boundaries in digital environments (Hong & Thong, 2013).

To provide a comprehensive explanation of privacy-related decision-making, Smith et al. (2011) proposed the Antecedents–Privacy Concerns–Outcomes (APCO) macro-model. In this framework, privacy concerns occupy a central position, linking antecedent factors (such as prior privacy experience, awareness, personality traits, and cultural differences) to behavioral outcomes. The APCO model has since become one of the most widely adopted frameworks for examining both the drivers and consequences of privacy concerns in information systems research (Harborth & Pape, 2021).

The APCO model is closely associated with the concept of privacy calculus, which conceptualizes individuals' disclosure decisions as a trade-off between perceived risks and perceived benefits (Kokolakis, 2017). Originating from behavioral calculus theory (Laufer & Wolfe, 1977), privacy calculus suggests that individuals are more likely to disclose personal information when perceived benefits outweigh potential risks. Within the APCO framework, this trade-off mechanism is embedded as part of a broader decision-making process, in which privacy concerns mediate the relationship between antecedent conditions and behavioral intentions.

However, the rationality assumption underlying privacy calculus has been increasingly questioned. The model assumes that users are able to systematically evaluate risks and benefits before making disclosure decisions. In practice, such assumptions may not hold. Due to cognitive limitations, time constraints, and information asymmetry, users often rely on simplified decision-making strategies rather than fully rational evaluation processes. Behavioral economics further suggests that factors such as uncertainty, ambiguity, and framing effects may influence users' decisions (Bahirat et al., 2018; Johnson et al., 2002). As a result, privacy-related behaviors may not always reflect deliberate or well-informed reasoning.

In addition, recent studies have argued that privacy decision-making is often neither fully informed nor the result of high cognitive effort (Dinev et al., 2015; Goes, 2013; Varian, 2009). In increasingly complex digital environments, users may lack the ability to fully understand how their personal data are collected, processed, and utilized. This limitation weakens the assumption of fully rational privacy calculus and suggests that privacy concerns may not always translate into corresponding behavioral responses.

Given these considerations, the APCO model provides a valuable theoretical lens for examining privacy-related behavior in the context of emerging digital payment technologies. In particular, it allows for the analysis of how users evaluate the trade-off between perceived risks and benefits when disclosing sensitive information. In the context of facial recognition payment, where highly sensitive biometric data are involved, privacy concerns are expected to play a central role in shaping users' behavioral intentions. Therefore, APCO serves as an appropriate framework for analyzing how privacy-related perceptions influence users' continuance behavior in this study.

Research on Behavioral Intentions of Facial Recognition Payment Users

With the rapid development and widespread application of facial recognition payment (FRP), research on user behavior in this domain has attracted increasing attention. Existing studies can generally be categorized into pre-adoption and post-adoption research. A systematic review shows that most prior studies focus on pre-adoption behavior, particularly users' intention to adopt or use FRP.

Pre-adoption studies are predominantly grounded in technology acceptance theories, including the Technology Acceptance Model (TAM) (Dang et al., 2022; Hizam et al., 2021; Liao et al., 2022; Zhang & Kang, 2019), the Theory of Planned Behavior (TPB) (Hwang et al., 2024; Wu et al., 2024), and the Unified Theory of Acceptance and Use of Technology (UTAUT) (Moriuchi, 2021; Nan et al., 2022). In addition, scholars have incorporated complementary perspectives such as perceived value theory, protection motivation theory, trust theory, innovation resistance, and theory of mind to construct extended analytical frameworks. These studies have significantly enriched the understanding of factors influencing users' initial adoption of FRP.

As FRP technologies become more mature and widely used, the importance of post-adoption behavior has become increasingly evident. Compared with initial adoption, continuance intention is more critical for the long-term success and sustainability of a technology. Accordingly, a growing number of studies have begun to examine post-adoption behavior, which can be broadly divided into continuance behavior and resistance behavior.

From a process perspective, user behavior can be understood as dynamic and stage-based. In the early stage of technology diffusion, research on adoption intention helps reduce barriers and facilitates initial acceptance. As the technology becomes widely adopted, users may develop concerns or hesitation regarding continued use. At this stage, research should focus on continuance intention, since directly examining resistance behavior without considering this stage may limit the explanation of sustained usage mechanisms and weaken the predictive power of user behavior models.

Although a limited number of studies have examined the continuance behavior of FRP users, their findings remain fragmented. Zhong and Moon (2022) found that perceived usefulness, perceived ease of use, and service security influence perceived value and user satisfaction, which subsequently promote continuance behavior and word-of-mouth intention, although perceived value does not directly affect continuance intention. Li and Li (2023) showed that trust in both the service provider and the FRP system positively affects continuance intention, while perceived security enhances trust. Lee and Pan (2023) demonstrated that system attributes such as relative advantage, compatibility, interface attractiveness, and perceived security influence users' cognitive and emotional responses, which in turn drive continuance intention. Gao et al. (2023) found that perceived information vulnerability increases users' fear of financial loss and reputational damage, thereby reducing continuance intention, while transparency and fairness mechanisms mitigate these negative effects.

Despite these contributions, several limitations remain. First, existing studies on FRP continuance behavior have not sufficiently linked post-adoption behavior with users' pre-adoption perceptions. In particular, the roles of expectation confirmation and post-usage perceived usefulness in shaping satisfaction and continuance intention have not been systematically examined. Second, prior research has not adequately incorporated privacy-related factors into post-adoption models, which limits the ability to explain the coexistence of high privacy concerns and continued usage.

To address these gaps, this study integrates the Expectation Confirmation Model (ECM) with the privacy calculus perspective within the APCO framework to develop a comprehensive model of continuance behavior. Specifically, the study examines how users' pre-adoption expectations are confirmed through actual use, how privacy-related perceptions influence post-adoption evaluations, and how these factors jointly shape continuance intention in the context of facial recognition payment in China.

Accordingly, the research framework adopted in this study is depicted in Figure 1.

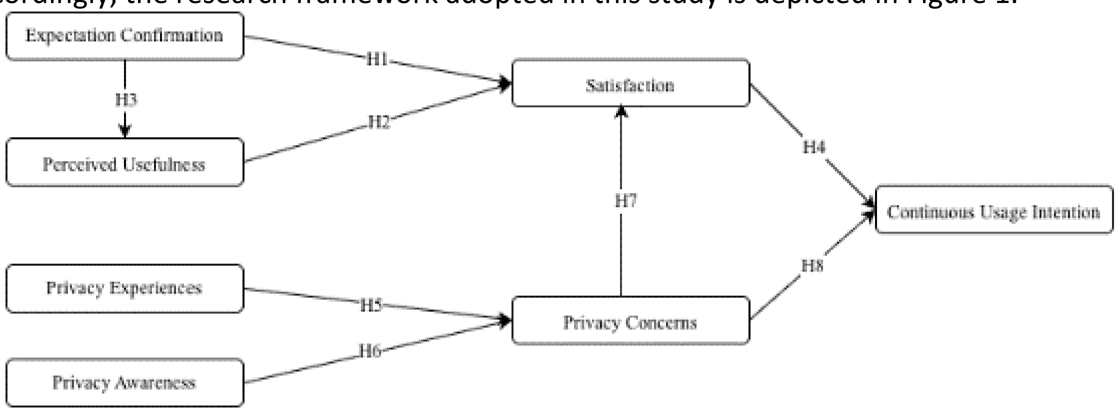

Figure1. The Framework of Research

Development of Hypothesis

Expectation Confirmation

Expectation confirmation refers to users' evaluation of whether their initial expectations are met after actual use of a system. Within the Expectation Confirmation Model (ECM), confirmation is proposed to have a positive effect on both perceived usefulness and user satisfaction (Bhattacherjee, 2001b). When users perceive that their expectations are fulfilled through actual experience, they are more likely to evaluate the system as useful and develop a higher level of satisfaction.

Empirical evidence has consistently supported these relationships across various information systems contexts. For example, prior studies have confirmed the positive effects of expectation confirmation on perceived usefulness and satisfaction in mobile shopping (Shang & Wu, 2017), mobile banking (Yuan et al., 2016), mobile applications (Tam et al., 2020), smartphone banking services (Susanto et al., 2016), and wearable technologies such as smartwatches (Ogbanufe & Gerhart, 2018). In addition, meta-analytic findings further validate the robustness of these relationships across different technological settings (Ambalov, 2018).

In the context of facial recognition payment, when users perceive that the actual performance of the technology aligns with or exceeds their prior expectations, they are more likely to form positive evaluations of its usefulness and experience greater satisfaction. Therefore, the following hypotheses are proposed:
H1: Expectation confirmation positively influences users' perceived usefulness of facial recognition payment.
H2: Expectation confirmation positively influences users' satisfaction with facial recognition payment.

Perceived Usefulness

In the technology adoption literature, perceived usefulness has long been recognized as a key determinant of users' attitudes and behavioral intentions toward technology (Davis et al., 1989). Although perceived ease of use is also important in the initial adoption stage, prior research suggests that its role becomes less salient in the post-adoption stage. In contrast, perceived usefulness remains a stable and significant predictor of continuance-related outcomes (Bhattacherjee & Lin, 2015). Originally, perceived usefulness was defined as the extent to which an individual believes that using a particular system will enhance his or her performance (Davis et al., 1989). In later models, such as the Unified Theory of Acceptance and Use of Technology, this concept is closely related to performance expectancy (Venkatesh et al., 2003).

Within the Expectation Confirmation Model, perceived usefulness is proposed to positively influence user satisfaction (Bhattacherjee, 2001b). When users perceive that a system is beneficial and effective in meeting their needs, they are more likely to develop favorable post-usage evaluations and experience a higher level of satisfaction. This relationship has been supported in a range of post-adoption contexts. For example, prior studies have found that perceived usefulness positively affects satisfaction in the use of smartwatches (Ogbanufe and Gerhart, 2018) and smartphone banking services (Susanto et al., 2016).

In the context of facial recognition payment, users who perceive the technology as useful are more likely to evaluate their usage experience positively and feel satisfied with the service. Therefore, the following hypothesis is proposed:
H3: Perceived usefulness positively influences users' satisfaction with facial recognition payment.

Satisfaction
According to the Expectation Confirmation Model (ECM), satisfaction is a central determinant of continuance intention and a key driver of users' sustained engagement with information systems (Bhattacherjee, 2001b). Satisfaction is commonly defined as a post-consumption evaluative judgment in which users compare their perceived performance of a product or service with prior expectations (Westbrook & Oliver, 1991). In the context of information systems, satisfaction reflects users' overall evaluation of their usage experience after interacting with a system.

Extensive empirical evidence has confirmed the positive relationship between satisfaction and continuance intention across various technological contexts, including mobile services, banking systems, and wearable technologies (Ogbanufe and Gerhart, 2018; Shin et al., 2017; Susanto et al., 2016; Yuan et al., 2016). When users develop a higher level of satisfaction based on their actual experience, they are more likely to continue using the system over time. In the context of facial recognition payment, users who are satisfied with their usage experience are more likely to maintain their usage behavior and exhibit stronger continuance intention. Therefore, the following hypothesis is proposed:
H4: Satisfaction positively influences users' continuance intention toward facial recognition payment.

Privacy Experience
Privacy experience refers to individuals' prior exposure to privacy-related incidents, such as data breaches or misuse of personal information. Such experiences play a critical role in shaping users' perceptions of privacy risks. Individuals who have previously encountered privacy violations are more likely to develop heightened sensitivity toward potential threats and to reassess the risks associated with disclosing personal information (Gu et al., 2017).
Prior research suggests that accumulated privacy experiences, particularly those associated with negative emotions, can significantly increase users' level of privacy concerns (Acquisti et al., 2015). In contrast, individuals without such experiences may underestimate potential risks due to a lack of direct awareness. In the context of facial recognition payment, where users are required to provide highly sensitive biometric data, prior privacy experiences may further intensify users' concerns about the potential misuse of facial information. Users who have experienced privacy violations are more likely to perceive higher risks and exhibit stronger concerns regarding the disclosure of facial data. Empirical evidence supports the positive relationship between privacy experience and privacy concerns (Cheng et al., 2024). Therefore, the following hypothesis is proposed:
H5: Privacy experience positively influences users' privacy concerns.

Privacy Awareness
Privacy awareness refers to individuals' understanding of privacy issues as well as their knowledge of how organizations collect, use, and protect personal information (Smith et al.,

2011). A higher level of privacy awareness enables users to better recognize the importance of their personal data and the potential consequences of privacy breaches. As a result, users who are more aware of privacy issues are more likely to develop stronger concerns about the disclosure and use of sensitive information.

Prior research suggests that users with greater privacy awareness tend to be more cautious about information disclosure and more sensitive to potential privacy risks. For example, Culnan (1995) found that consumers with lower awareness of privacy-related practices were generally less concerned about privacy than those with higher privacy awareness. In the context of facial recognition payment, facial data are closely linked to users' payment accounts and personal identity, which makes privacy awareness particularly important. Users who are more aware of the sensitivity of facial information and the possible consequences of misuse are therefore more likely to express stronger privacy concerns. Accordingly, the following hypothesis is proposed:
H6: Privacy awareness positively influences users' privacy concerns.

Privacy Concerns
Privacy concerns are commonly conceptualized as individuals' general worries about the potential loss or misuse of personal information (Malhotra et al., 2004). In context-specific research, privacy concerns are further defined as users' apprehension that disclosing information to a particular external entity may result in a loss of privacy (Xu et al., 2011). In the context of facial recognition payment, privacy concerns refer to users' worries that providing facial information to FRP service providers may expose them to privacy risks, such as unauthorized disclosure, inappropriate secondary use, or sharing with third parties without consent.

These concerns are particularly salient in FRP settings because facial data are highly sensitive, permanent, and closely linked to users' identity and payment information. When users perceive that service providers may collect or use such data inappropriately, they are more likely to develop negative evaluations of the service. Prior studies have shown that privacy concerns can weaken users' willingness to engage with digital services and reduce their intention to continue using them (Liu et al., 2023; Owusu et al., 2020). In other words, heightened privacy concerns may undermine users' confidence in the service experience and discourage sustained usage.

In the context of facial recognition payment, users who are more concerned about privacy are likely to evaluate the service less favorably and become less willing to continue using it. Accordingly, the following hypothesis is proposed:
H7: Privacy concerns negatively influence users' satisfaction with facial recognition payment.
H8: Privacy concerns negatively influence users' continuance intention toward facial recognition payment.

Methodology
The primary objective of this study is to systematically examine the key factors influencing Chinese users' continuance intention toward facial recognition payment (FRP) and to explore the relationships among these variables. To achieve this goal, a quantitative research approach was adopted, with the target population consisting of Chinese FRP users aged 18

and above. To test the proposed research model and hypotheses, this study employed Partial Least Squares Structural Equation Modeling (PLS-SEM) for data analysis and model evaluation.
The minimum required sample size was estimated using G*Power. The results indicated that at least 107 valid responses were required to achieve sufficient statistical power.

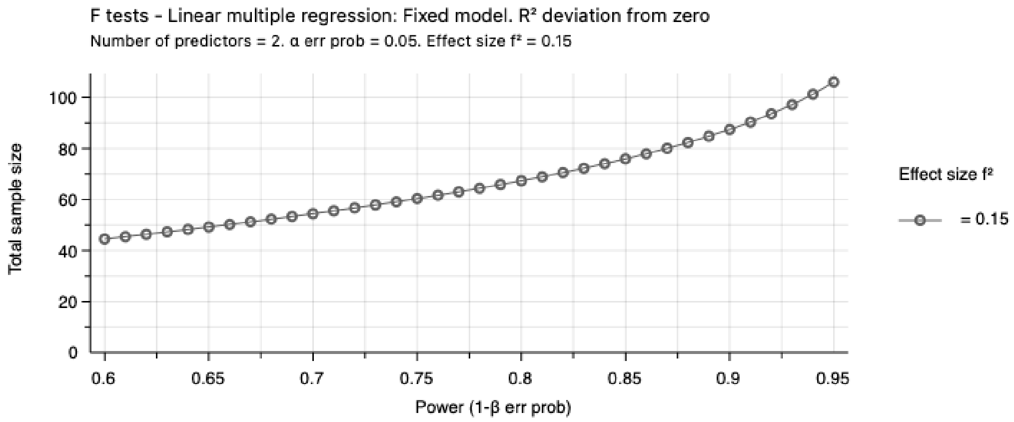

Figure 2. The Result of G*Power

The measurement items for each construct in the research framework were adapted from well-established studies, and the corresponding sources are presented in Table 1. All constructs were measured using a seven-point Likert scale.

Table 1.
Research Measurement Instrument

Constructs/items	No. of Items	Sources
Expectation Confirmation (EC)	3	(Bhattacherjee, 2001b)
Perceived Usefulness (PU)	4	(Zhong & Moon, 2022)
Satisfaction (SAT)	4	(Zhong & Moon, 2022)
Privacy Experience (PEX)	4	(Ioannou et al., 2020)
Privacy Awareness (PAW)	3	(Xu et al., 2011)
Privacy Concerns (PCON)	4	(Xu et al., 2011)
Continuous Usage Intention (CUI)	3	(Bhattacherjee, 2001b)
Maker Variable (MV)	3	(Lin et al., 2015)

The data for this study were collected through a self-administered questionnaire using the Credamo online survey platform (Data and Model Creator, www.credamo.com). During the data collection process, the platform implemented a series of strict quality control procedures, including PC uniqueness checks (to prevent duplicate submissions based on username and IP address) and a mechanism that prevents the submission of incomplete questionnaires. In addition, the platform provides reliable data, and its survey data have been widely used in several international peer-reviewed journals.

In total, 382 responses were initially collected. After data screening and cleaning, 369 valid questionnaires were retained for analysis. The final sample size exceeded the minimum required threshold, ensuring the robustness of the subsequent statistical analyses.
Statistical analyses were performed using SPSS 28.0 and SmartPLS 4.0. SPSS was used for data screening and cleaning, followed by descriptive analysis and hypothesis testing. The analysis was conducted in two stages. First, the measurement model was assessed. Reliability and validity were evaluated using composite reliability, average variance extracted (AVE), and the heterotrait–monotrait ratio (HTMT) to establish convergent and discriminant validity.

Second, the structural model was examined after the measurement model met the required criteria. Bootstrapping with 10,000 resamples was applied to test the significance of path coefficients. In addition, the coefficients of determination (R^2) and effect sizes (f^2) were analyzed to evaluate the model's explanatory power and the relative impact of the antecedent variables.

Ethical Considerations
Participation in this study was entirely voluntary, and only individuals capable of providing informed consent were included. Participants were informed of their rights prior to participation. The study focused solely on the investigation of human behavior and did not involve any experimental intervention with human or animal subjects. No personally identifiable or sensitive information, such as names, contact details, or residential addresses, was collected.

The Results
Demographic Profile
A total of 369 valid responses were included in the final analysis. The demographic characteristics of the respondents are presented in Table 2.
In terms of gender distribution, the sample was relatively balanced, with 190 female respondents (51.5%) and 179 male respondents (48.5%). Regarding age, the majority of respondents were between 32 and 45 years old (46.1%), followed by those aged 18 to 31 (42.8%). A smaller proportion of participants were aged 46 to 61 (9.5%), while respondents over 62 years old accounted for only 1.6%, indicating that the sample was predominantly composed of young and middle-aged users.

With respect to educational background, most respondents held a bachelor's degree (65.9%), followed by master's degree holders (16.8%). Participants with diploma or vocational education accounted for 11.1%, while those with high school education or below represented 4.9%. Doctoral degree holders comprised a small proportion of the sample (1.4%). This suggests that the sample was generally well-educated.

In terms of occupation, the majority of respondents were company employees (70.7%), followed by students (13.3%) and government or public sector employees (9.8%). Other occupational categories, including self-employed individuals (4.6%), retirees (0.5%), homemakers (0.3%), and other occupations (0.8%), represented relatively small proportions. Regarding usage experience, more than half of the respondents (53.9%) reported using facial recognition payment for more than two years, while 26.8% had used it for one to two years. Smaller proportions reported shorter usage durations, including 6–12 months (8.9%), 1–6 months (4.1%), and less than one month (4.6%), while 1.6% could not recall their usage duration. These results indicate that most participants were experienced users of facial recognition payment.

In terms of usage frequency, the largest group of respondents reported using facial recognition payment several times a week (4–6 times) (36.0%), followed by daily or almost daily users (26.0%) and those using it occasionally each week (1–3 times) (25.7%). A smaller proportion reported occasional monthly use (9.8%), while only 2.4% used it rarely. This suggests that facial recognition payment has become a frequently used payment method among the respondents.

Table 2
The Details of Profile

Characteristics	Frequency	Percentage (%)
Gender		
Female	190	51.5
Male	179	48.5
Age		
Over 62 years old	6	1.6
46–61 years old	35	9.5
32-45 years old	170	46.1
18-31 years old	158	42.8
Education		
Bachelor’s degree	243	65.9
Diploma / Vocational education	41	11.1
Doctoral degree	5	1.4
High school or below	18	4.9
Master’s degree	62	16.8
Occupation		
Company employee	261	70.7
Government or public sector employee	36	9.8
Homemaker	1	0.3
Other	3	0.8
Retired	2	0.5
Self-employed / Freelancer	17	4.6
Student	49	13.3
Duration of use		
1–2 years	99	26.8
1–6 months	15	4.1

6–12 months	33	8.9
Cannot recall	6	1.6
Less than 1 month	17	4.6
More than 2 years	199	53.9
Frequency of use		
Daily or almost daily	96	26
Occasionally each month (1–3 times)	36	9.8
Occasionally each week (1–3 times)	95	25.7
Rarely (less than once per month)	9	2.4
Several times a week (4–6 times)	133	36
Total	**369**	

Common Method Variance (CMV)
Common method variance (CMV) refers to bias arising when variables are measured using the same method or data source (Richardson et al., 2009). This issue may occur when respondents evaluate both independent and dependent variables within a single survey at the same point in time (Podsakoff et al., 2003).

To assess and mitigate the potential impact of CMV, a marker variable approach was employed (Lindell & Whitney, 2001). Specifically, a marker variable consisting of three items adapted from Oreg (2003) was included in the questionnaire. The results indicated that the differences in R^2 values ranged from 0% to 1%. As these differences were well below the recommended threshold of 10%, CMV is unlikely to pose a significant concern in this study.

Assessment of Measurement Model
The measurement model was first assessed in terms of reliability and validity. Convergent validity was evaluated using average variance extracted (AVE), while composite reliability (CR) was used to assess internal consistency. As shown in Table 3, all AVE values exceeded the recommended threshold of 0.50, and all CR values were above 0.70, indicating satisfactory convergent validity and reliability (Hair & Alamer, 2022; Ramayah et al., 2018).

Discriminant validity was examined using the heterotrait–monotrait ratio (HTMT), following the criterion proposed by Franke and Sarstedt (2019). As reported in Table 4, most HTMT values were below the recommended threshold of 0.90, suggesting adequate discriminant validity. Although three pairs of constructs showed HTMT values slightly above 0.90, specifically satisfaction and expectation confirmation (0.935), and satisfaction and perceived usefulness (0.928), further assessment was conducted using bootstrapped confidence intervals at the 90% level.

The results indicated that all upper confidence interval limits were below 1.00. According to the recommendations of Franke and Sarstedt (2019), these findings confirm that discriminant validity is established and does not pose a concern in this study.

Table 3
Measurement Model

Variables	Items	Outer loadings	Composite reliability	AVE
Continuous Usage Intention (CUI)	**CUI1**	0.800	0.879	0.644
	CUI2	0.751		
	CUI3	0.828		
	CUI4	0.831		
Expectation Confirmation (EC)	**EC1**	0.798	0.797	0.567
	EC2	0.753		
	EC3	0.706		
Privacy Awareness (PAW)	**PAW1**	0.839	0.950	0.791
	PAW2	0.901		
	PAW3	0.901		
	PAW4	0.906		
	PAW5	0.898		
Privacy Concerns (PCON)	**PCON1**	0.931	0.969	0.864
	PCON2	0.923		
	PCON3	0.939		
	PCON4	0.942		
	PCON5	0.912		
Privacy Experience (PEX)	**PEX1**	0.906	0.950	0.864
	PEX2	0.952		
	PEX3	0.929		
Perceived Usefulness (PU)	**PU1**	0.685	0.776	0.536
	PU3	0.729		
	PU4	0.780		
Satisfaction (SAT)	**SAT1**	0.782	0.840	0.567
	SAT2	0.774		
	SAT3	0.726		
	SAT4	0.728		

Note: The PU2 (0.548) was deleted due to low loading.

Table 4
Discriminant Validity (HTMT)

	CUI	EC	PAW	PCON	PEX	PU	SAT
CUI							
EC	0.730						
PAW	0.404	0.312					
PCON	0.576	0.336	0.540				
PEX	0.081	0.077	0.102	0.235			
PU	0.876	0.678	0.277	0.436	0.154		
SAT	0.867	0.935	0.313	0.413	0.184	0.928	

Assessment of Structural Model

Following the satisfactory assessment of the measurement model, the structural model was evaluated to test the proposed hypotheses. A bootstrapping procedure with 10,000 resamples was employed to assess the significance of the path coefficients, and the results are presented in Table 5.

The findings indicate that most of the hypothesized relationships are statistically significant. Specifically, within the ECM framework, expectation confirmation (EC) has a significant positive effect on satisfaction (SAT) ($\beta = 0.447$, $t = 10.088$, $p < 0.001$), supporting H1. Expectation confirmation (EC) also has a significant positive effect on perceived usefulness (PU) ($\beta = 0.405$, $t = 6.478$, $p < 0.001$), supporting H3. In addition, perceived usefulness (PU) significantly and positively influences satisfaction (SAT) ($\beta = 0.399$, $t = 10.334$, $p < 0.001$), supporting H2. Satisfaction (SAT), in turn, exerts a strong positive effect on continuance intention (CUI) ($\beta = 0.574$, $t = 10.595$, $p < 0.001$), supporting H4. These results highlight the central role of satisfaction in explaining users' continuance behavior.

Regarding the privacy-related paths, privacy experience (PEX) has a significant positive effect on privacy concerns (PCON) ($\beta = 0.271$, $t = 6.148$, $p < 0.001$), supporting H5. However, privacy awareness (PAW) shows a significant negative effect on privacy concerns (PCON) ($\beta = -0.543$, $t = 12.899$, $p < 0.001$), which is inconsistent with the hypothesized direction. Therefore, H6 is not supported. Furthermore, privacy concerns (PCON) negatively influence satisfaction (SAT) ($\beta = -0.106$, $t = 2.730$, $p = 0.003$), supporting H7, and also have a significant negative effect on continuance intention (CUI) ($\beta = -0.313$, $t = 7.548$, $p < 0.001$), supporting H8. These findings suggest that higher levels of perceived privacy risk reduce users' satisfaction and weaken their intention to continue using FRP.

In terms of effect size, satisfaction (SAT) has a substantial effect on continuance intention (CUI) ($f^2 = 0.647$). Expectation confirmation (EC) and perceived usefulness (PU) exhibit moderate to large effects on satisfaction (SAT) ($f^2 = 0.376$ and 0.287, respectively). Privacy awareness (PAW) also demonstrates a relatively strong effect on privacy concerns (PCON) ($f^2 = 0.447$), while the remaining relationships show small to moderate effect sizes. These results indicate that both ECM-related and privacy-related factors play important roles in the model. Additionally, all variance inflation factor (VIF) values are below the threshold of 5, indicating no multicollinearity issues. The confidence intervals for all paths do not include zero, further confirming the robustness of the results.

Overall, the structural model demonstrates strong explanatory power, with both utilitarian factors and privacy-related factors jointly influencing users' continuance intention toward facial recognition payment.
To further evaluate the predictive capability of the model, the PLS-Predict procedure was conducted. The predictive relevance of the model was first assessed using Q^2_predict values. As shown in Table 6, all Q^2_predict values for the endogenous construct (CUI) are greater than zero, ranging from 0.149 to 0.238. This indicates that the model has adequate predictive relevance for the indicators (Shmueli et al., 2019).

Next, the predictive performance of the PLS-SEM model was compared with a linear model (LM) and a simple indicator average (IA) benchmark using root mean squared error (RMSE) values. The results show that for most indicators (CUI1, CUI2, and CUI3), the RMSE values of the PLS-SEM model are lower than those of both the LM and IA models. Although for CUI4 the RMSE of PLS-SEM is slightly higher than that of the LM model, it remains lower than that of the IA benchmark.

Furthermore, the differences in prediction errors (PLS-LM and PLS-IA) are predominantly negative, indicating that the PLS-SEM model generally produces lower prediction errors than the benchmark models. According to the guidelines proposed by Shmueli et al. (2019), these results suggest that the model demonstrates medium to high predictive power.
Overall, the findings confirm that the proposed model not only exhibits strong explanatory capability but also possesses satisfactory out-of-sample predictive performance.

Table 5
Hypotheses Testing

Hypothesis	Relationships	Std. Beta	Std. Dev.	T values	P values	PCL LL	PCL UL	f^2	VIF	Decision
H1	**EC -> SAT**	0.447	0.044	10.088	0.000	0.371	0.516	0.376	1.224	Supported
H2	**PU -> SAT**	0.399	0.039	10.334	0.000	0.338	0.465	0.287	1.279	Supported
H3	**EC -> PU**	0.405	0.063	6.478	0.000	0.300	0.506	0.196	1.000	Supported
H4	**SAT -> CUI**	0.574	0.054	10.595	0.000	0.477	0.655	0.647	1.145	Supported
H5	**PEX -> PCON**	0.271	0.044	6.148	0.000	0.199	0.344	0.111	1.007	Supported
H6	**PAW -> PCON**	-0.543	0.042	12.899	0.000	-0.613	-0.474	0.447	1.007	Not Supported
H7	**PCON -> SAT**	-0.106	0.039	2.730	0.003	-0.169	-0.040	0.022	1.150	Supported
H8	**PCON -> CUI**	-0.313	0.041	7.548	0.000	-0.384	-0.246	0.193	1.145	Supported

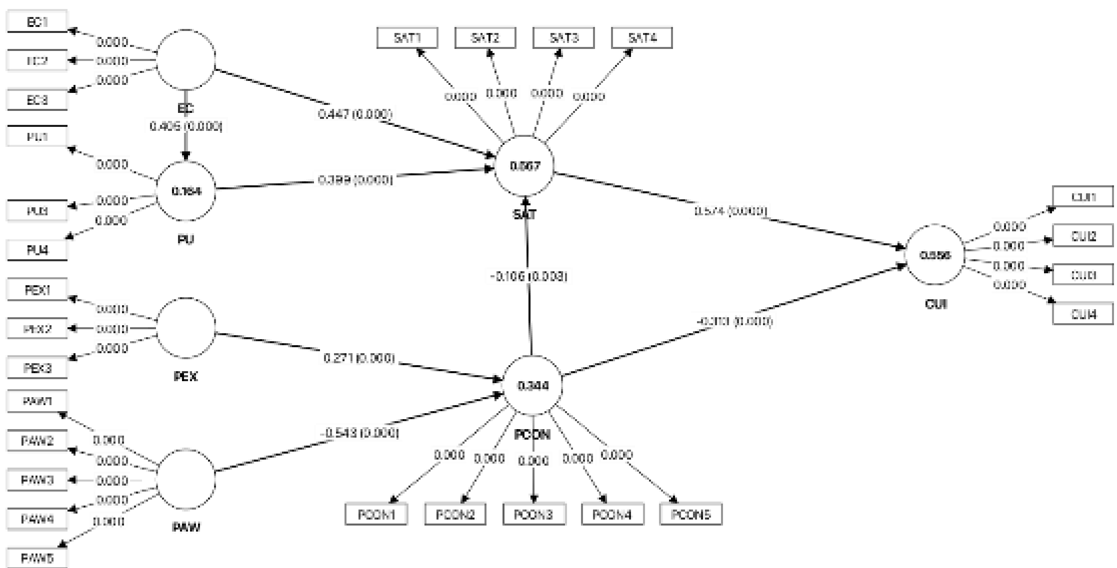

Figure 3. Assessment of Structural Model

Table 6
PLS-predict

Items	Q^2predict	PLS-SEM_RMSE	LM_RMSE	IA_RMSE	PLS-LM	PLS-IA
CUI1	0.149	0.902	0.924	0.978	-0.022	-0.076
CUI2	0.158	0.892	0.903	0.972	-0.011	-0.080
CUI3	0.209	1.028	1.048	1.156	-0.020	-0.128
CUI4	0.238	0.991	0.982	1.136	0.009	-0.145

Discussion

This study integrates the ECM and the APCO framework to examine the factors influencing Chinese users' continuance intention toward facial recognition payment (FRP). The findings provide important insights into both utilitarian and privacy-related mechanisms underlying post-adoption behavior.

First, the results support the core propositions of ECM. Expectation confirmation significantly enhances both perceived usefulness and satisfaction, indicating that when users' actual experiences meet or exceed their initial expectations, they are more likely to develop positive evaluations of the technology. This finding is consistent with Bhattacherjee (2001) and highlights the importance of expectation confirmation in the post-adoption stage. In addition, perceived usefulness has a significant positive effect on satisfaction, suggesting that users who perceive FRP as efficient and convenient are more likely to report favorable usage experiences. Furthermore, satisfaction exerts a strong positive influence on continuance intention, confirming its central role in driving sustained usage behavior.

Second, with regard to privacy-related factors, the findings show that privacy experience positively influences privacy concerns. This suggests that users who have previously encountered privacy violations are more sensitive to potential risks and are more likely to express heightened concerns about the misuse of personal data. This result is consistent with prior research, which emphasizes the role of past experiences in shaping individuals' risk perceptions.

However, contrary to the proposed hypothesis, privacy awareness has a significant negative effect on privacy concerns. This unexpected result reveals a counterintuitive pattern and has important theoretical implications. While previous research generally assumes that higher levels of privacy awareness lead to stronger privacy concerns, the present study suggests that this relationship may not hold in highly embedded technological contexts such as FRP in China. One possible explanation is that as FRP becomes deeply integrated into everyday life, users gradually become familiar with and reliant on the technology, leading to a process of risk normalization. Even when users are aware of potential privacy risks, repeated exposure and habitual use may reduce their perceived severity. In addition, users with higher privacy awareness may possess greater knowledge and cognitive ability to evaluate platform security mechanisms, which may enhance their confidence in the system and, consequently, reduce their level of concern. Moreover, in high-frequency usage scenarios, users are likely to engage in a rational trade-off between convenience and risk, which may further attenuate their sensitivity to privacy issues.

Further analysis shows that privacy concerns have a significant negative effect on both satisfaction and continuance intention, indicating that perceived privacy risks still play an important role in shaping users' evaluations and behavioral intentions. However, it is noteworthy that the positive effect of satisfaction on continuance intention ($\beta = 0.574$) is substantially stronger than the negative effect of privacy concerns ($\beta = -0.313$). This finding suggests that utilitarian benefits dominate users' decision-making in the context of FRP.

In other words, although users are aware of potential privacy risks, these concerns do not exert a decisive inhibitory effect on their continuance behavior. Instead, users appear to prioritize the convenience and efficiency provided by FRP, while tolerating or rationalizing privacy risks to some extent. This reflects a benefit-driven decision pattern in which perceived benefits outweigh perceived risks, thereby encouraging continued usage despite existing privacy concerns.

Taken together, these findings reveal a typical manifestation of the “privacy paradox,” where users express concerns about privacy yet continue to engage with the technology. This paradox suggests that user behavior is not solely driven by rational risk avoidance but is shaped by a combination of perceived benefits, habitual use, and the degree of technological embeddedness.

Overall, this study contributes to the literature by demonstrating that both utilitarian and privacy-related factors jointly influence continuance intention. By integrating ECM and APCO, the study extends the explanatory power of both models and provides a more comprehensive understanding of user behavior in the context of facial recognition payment in China.

Theoretical Implication

This study makes several important theoretical contributions to the literature on information systems continuance and privacy-related behavior.

First, it extends the Expectation Confirmation Model to the context of facial recognition payment. By confirming the effects of expectation confirmation, perceived usefulness, and satisfaction on continuance intention, the study demonstrates that ECM remains effective in explaining post-adoption behavior in emerging biometric payment settings.

Second, it broadens the application of the APCO framework by showing that privacy-related factors continue to matter after adoption. Specifically, privacy concerns significantly reduce both satisfaction and continuance intention, indicating that privacy remains a relevant factor in ongoing technology use rather than only in initial adoption.

Third, by integrating ECM and APCO, this study offers a more comprehensive explanation of continuance behavior. This combined framework captures both utilitarian evaluations and privacy-related considerations, providing a more complete understanding of how users assess FRP after adoption.

Fourth, the findings contribute to the privacy paradox literature. Although privacy concerns negatively affect continuance intention, their influence is weaker than the positive effect of satisfaction. This suggests that users do not ignore privacy risks, but continue using FRP because perceived benefits outweigh perceived risks. In addition, the negative relationship between privacy awareness and privacy concerns challenges the common assumption that awareness necessarily increases concern, and suggests that familiarity, trust, or risk normalization may shape privacy perceptions in mature usage contexts.

Managerial Implications

This study also provides several practical implications for service providers, platform operators, and policymakers involved in facial recognition payment systems.

First, service providers should prioritize user satisfaction, as it is the strongest predictor of continuance intention. Improving recognition accuracy, transaction speed, and system stability can help ensure that user expectations are met.

Second, providers should continue to emphasize the functional value of FRP, especially convenience and efficiency, as these benefits play a dominant role in continued use.
Third, privacy concerns still significantly reduce satisfaction and continuance intention. Therefore, providers should strengthen data protection measures, improve transparency in data use, and reduce users' perceived privacy risks.

Finally, policymakers should establish clearer and stricter regulations for biometric data governance. Because facial data are highly sensitive and irreversible, stronger legal protections are essential for promoting user trust and supporting the sustainable development of FRP systems.

Conclusion

This study investigates the factors affecting Chinese users' intention to continue using facial recognition payments by combining the ECM and the APCO framework. The findings indicate that satisfaction mainly influences continuance intention, whereas privacy concerns have a notable but comparatively weaker negative impact.

By integrating utilitarian and privacy-related perspectives, this study offers a more comprehensive understanding of post-adoption behaviour in digital payment contexts. The findings also provide empirical support for the privacy paradox, demonstrating that users continue to adopt and use FRP despite being aware of potential privacy risks. Additionally, the unexpected negative relationship between privacy awareness and privacy concerns emphasises the importance of contextual factors such as familiarity and habitual use.

Overall, this study contributes to both theory and practice by explaining how users balance perceived benefits and risks in the continued use of facial recognition payment.

Theoretical and Contextual Contribution

Beyond the empirical findings, this study provides important theoretical and contextual contributions. Theoretically, it enhances the information systems literature by integrating the ECM with the APCO framework to explain post-adoption behaviour. This integration offers a more comprehensive account of continuance intention by simultaneously capturing utilitarian evaluations and privacy-related considerations, thereby building on prior research that has typically examined these dimensions separately. In particular, the study contributes to the privacy paradox literature by demonstrating how the coexistence of high privacy concerns and ongoing usage can be explained through a benefit–risk trade-off mechanism in a post-adoption context.

This study offers evidence from China, one of the most advanced and large-scale markets for facial recognition payments. The findings emphasise how technological integration, frequent usage, and platform maturity influence users' perceptions and behaviours differently from those in Western settings. By demonstrating that privacy awareness may decrease, rather than heighten, privacy concerns in this context, the study provides a nuanced understanding of user cognition in highly digitalised environments. Consequently, it not only enhances the global discussion on digital payment adoption but also delivers context-specific insights for emerging economies experiencing rapid digital transformation.

Limitations and Directions for Future Studies

Despite its contributions, this study has a number of limitations that should be recognised. First, this study employed a cross-sectional research design, which limits the ability to capture dynamic changes in users' perceptions and behavior over time. Future research could adopt longitudinal designs to examine how continuance intention evolves over the prolonged use of facial recognition payments.

Second, the sample was limited to Chinese users, which may affect the generalizability of the findings. Given that cultural and regulatory environments differ across regions, future research could conduct cross-cultural comparisons to examine whether the observed relationships hold in other contexts.

Finally, this study focused on key constructs derived from the ECM and the APCO framework. Future research could extend the model by incorporating additional factors, such as trust, perceived risk dimensions, or institutional mechanisms, to further enrich the understanding of continuance behavior in biometric payment systems.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509-514. https://doi.org/10.1126/science.aaa1465

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179-211.

Al-Sharafi, M. A., Al-Qaysi, N., Iahad, N. A., & Al-Emran, M. (2022). Evaluating the sustainable use of mobile payment contactless technologies within and beyond the COVID-19 pandemic using a hybrid SEM-ANN approach. *International Journal of Bank Marketing*, *40*(5), 1071-1095. https://doi.org/10.1108/IJBM-07-2021-0291

Ambalov, I. A. (2018). A meta-analysis of IT continuance: An evaluation of the expectation-confirmation model. *Telematics and Informatics*, *35*(6), 1561-1571. https://doi.org/10.1016/j.tele.2018.03.016

Bahirat, P., Sun, Q., & Knijnenburg, B. P. (2018). Scenario context V/s framing and defaults in managing privacy in household IoT. Companion Proceedings of the 23rd International Conference on Intelligent User Interfaces,

Bhattacherjee, A. (2001a). An empirical analysis of the antecedents of electronic commerce service continuance. *Decision Support Systems*, *32*(2), 201-214. https://doi.org/10.1016/S0167-9236(01)00111-7

Bhattacherjee, A. (2001b). Understanding information systems continuance: An expectation-confirmation model. *MIS Quarterly*, 351-370. https://doi.org/10.2307/3250921

Bhattacherjee, A., & Lin, C.-P. (2015). A unified model of IT continuance: Three complementary perspectives and crossover effects. *European Journal of Information Systems*, *24*(4), 364-373. https://doi.org/10.1057/ejis.2013.36

Bhattacherjee, A., Perols, J., & Sanford, C. (2008). Information technology continuance: A theoretic extension and empirical test. *Journal of Computer Information Systems*, *49*(1), 17-26. https://doi.org/10.1080/08874417.2008.11645302

Bromberg, D. E., Charbonneau, É., & Smith, A. (2020). Public support for facial recognition via police body-worn cameras: Findings from a list experiment. *Government Information Quarterly*, *37*(1), 101415. https://doi.org/10.1016/j.giq.2019.101415

Chen, W., & Wang, M. (2023). Regulating the use of facial recognition technology across borders: A comparative case analysis of the European Union, the United States, and China. *Telecommunications Policy*, *47*(2), 102482. https://doi.org/10.1016/j.telpol.2022.102482

Cheng, E., & Shao, G. (2019). *Growing backlash in China against A.I. and facial recognition*. Retrieved Oct from https://www.cnbc.com/2019/09/06/ai-worries-about-the-dangers-of-facial-recognition-growing-in-china.html

Cheng, X., Qiao, L., Yang, B., & Zhang, X. (2024). Investigation on users' resistance intention to facial recognition payment: A perspective of privacy. *Electronic Commerce Research*, *24*(1), 275-301. https://doi.org/10.1007/s10660-022-09588-y

Chiu, W., Cho, H., & Chi, C. G. (2020). Consumers' continuance intention to use fitness and health apps: An integration of the expectation–confirmation model and investment model. *Information Technology & People*, *34*(3), 978-998. https://doi.org/10.1108/ITP-09-2019-0463

Collingridge, D. (1982). The social control of technology. *New York: St. Martin's Press*, 200. http://hdl.handle.net/10822/792071

Culnan, M. J. (1995). Consumer awareness of name removal procedures: Implications for direct marketing. *Journal of Direct Marketing*, *9*(2), 10-19. https://doi.org/10.1002/dir.4000090204

Dang, V. T., Nguyen, N., Nguyen, H. V., Nguyen, H., Van Huy, L., Tran, V. T., & Nguyen, T. H. (2022). Consumer attitudes toward facial recognition payment: An examination of antecedents and outcomes. *International Journal of Bank Marketing*, *40*(3), 511-535. https://doi.org/10.1108/IJBM-04-2021-0135

Dargan, S., & Kumar, M. (2020). A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities. *Expert Systems with Applications*, *143*, 113114. https://doi.org/10.1016/j.eswa.2019.113114

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, *35*(8), 982-1003. https://doi.org/10.1287/mnsc.35.8.982

Dinev, T., & Hart, P. (2005). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce*, *10*(2), 7-29. https://doi.org/10.1080/01449290410001715723

Dinev, T., McConnell, A. R., & Smith, H. J. (2015). Research commentary—informing privacy research through information systems, psychology, and behavioral economics: Thinking outside the "APCO" box. *Information Systems Research*, *26*(4), 639-655. https://doi.org/10.1287/isre.2015.0600

Ding, J. (2019). *ChinAI #77: A Strong Argument Against Facial Recognition in the Beijing Subway*. Retrieved Oct from https://chinai.substack.com/p/chinai-77-a-strong-argument-against

Esteban, V.-F., & Daniel, G.-J. (2016). Face recognition for authentication on mobile devices. *Image and Vision Computing*, *55*, 31-33. https://doi.org/10.1016/j.imavis.2016.03.018

Franke, G., & Sarstedt, M. (2019). Heuristics versus statistics in discriminant validity testing: A comparison of four procedures. *Internet Research*, *29*(3), 430-447. https://doi.org/10.1108/IntR-12-2017-0515

Gao, W., Guo, Q., & Jiang, N. (2023). Information vulnerability in facial recognition payment: An explanation of technology threat avoidance and information boundary theory. *Electronic Commerce Research and Applications*, *61*, 101298. https://doi.org/10.1016/j.elerap.2023.101298

Goes, P. B. (2013). Editor's comments: Information systems research and behavioral economics. *MIS Quarterly*, *37*(3), 3-8.

Gu, J., Xu, Y. C., Xu, H., Zhang, C., & Ling, H. (2017). Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decision Support Systems*, *94*, 19-28. https://doi.org/10.1016/j.dss.2016.10.002

Hair, J., & Alamer, A. (2022). Partial Least Squares Structural Equation Modeling (PLS-SEM) in second language and education research: Guidelines using an applied example. *Research Methods in Applied Linguistics*, *1*(3), 100027. https://doi.org/10.1016/j.rmal.2022.100027

Harborth, D., & Pape, S. (2021). Investigating privacy concerns related to mobile augmented reality Apps: A vignette based online experiment. *Computers in Human Behavior*, *122*, 106833. https://doi.org/10.1016/j.chb.2021.106833

Hizam, S. M., Ahmed, W., Fahad, M., Akter, H., Sentosa, I., & Ali, J. (2021). User behavior assessment towards biometric facial recognition system: A SEM-neural network approach. Advances in Information and Communication: Proceedings of the 2021 Future of Information and Communication Conference (FICC),

Hong, W., & Thong, J. Y. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly*, 275-298. http://www.jstor.org/stable/43825946

Hu, B., Liu, Y.-l., & Yan, W. (2023). Should I scan my face? The influence of perceived value and trust on Chinese users' intention to use facial recognition payment. *Telematics and Informatics*, *78*, 101951. https://doi.org/10.1016/j.tele.2023.101951

Hwang, J., Kim, J. S., Kim, H. M., & Kim, J. J. (2024). Effects of motivated consumer innovativeness on facial recognition payment adoption in the restaurant industry: A cross-cultural study. *International Journal of Hospitality Management*, *117*, 103646. https://doi.org/10.1016/j.ijhm.2023.103646

Ioannou, A., Tussyadiah, I., & Lu, Y. (2020). Privacy concerns and disclosure of biometric and behavioral data for travel. *International Journal of Information Management*, *54*, 102122. https://doi.org/10.1016/j.ijinfomgt.2020.102122

Johnson, E. J., Bellman, S., & Lohse, G. L. (2002). Defaults, framing and privacy: Why opting in-opting out. *Marketing Letters*, *13*, 5-15. https://doi.org/10.1023/A:1015044207315

Jones, A. (2020). *Biometrics: The Future of Payments? Global Payments Integrated*. Retrieved Septemper from https://www.globalpaymentsintegrated.com/en-us/blog/2020/06/30/biometrics-the-future-of-payments

Khalifa, M., & Liu, V. (2004). The state of research on information system satisfaction. *Journal of Information Technology Theory and Application (JITTA)*, *5*(4), 4. https://aisel.aisnet.org/jitta/vol5/iss4/4

Kim, J. J., Kim, I., & Hwang, J. (2021). A change of perceived innovativeness for contactless food delivery services using drones after the outbreak of COVID-19. *International*

Journal of Hospitality Management, *93*, 102758. https://doi.org/10.1016/j.ijhm.2020.102758

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122-134. https://doi.org/10.1016/j.cose.2015.07.002

Kostka, G., Steinacker, L., & Meckel, M. (2021). Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States. *Public Understanding of Science*, *30*(6), 671-690.

Kudina, O., & Verbeek, P.-P. (2019). Ethics from within: Google Glass, the Collingridge dilemma, and the mediated value of privacy. *Science, Technology, & Human Values*, *44*(2), 291-314.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues*, *33*(3), 22-42. https://doi.org/10.1111/j.1540-4560.1977.tb01880.x

Lee, C. T., & Pan, L.-Y. (2023). Smile to pay: predicting continuous usage intention toward contactless payment services in the post-COVID-19 era. *International Journal of Bank Marketing*, *41*(2), 312-332. https://doi.org/10.1108/IJBM-03-2022-0130

Lee, Y., & Kwon, O. (2011). Intimacy, familiarity and continuance intention: An extended expectation–confirmation model in web-based services. *Electronic Commerce Research and Applications*, *10*(3), 342-357. https://doi.org/10.1016/j.elerap.2010.11.005

Li, C., & Li, H. (2023). Disentangling facial recognition payment service usage behavior: A trust perspective. *Telematics and Informatics*, *77*, 101939. https://doi.org/10.1016/j.tele.2023.101939

Li, C., Li, H., & Wang, P. (2020). Facial payment use in China: An integrated view of privacy concerns and perceived benefits. Pacific Asia Conference on Information Systems,

Liao, M., Agnihotri, D., & Zhong, X. (2022). “Paying with my face”: Understanding users’ adoption and privacy concerns of facial recognition payment. Proceedings of the Human Factors and Ergonomics Society Annual Meeting,

Limedia. (2019). *2019 Facial Payment Research Report in China*. Retrieved September from https://www.theceomagazine.com/business/innovation-technology/facial

Lin, T.-C., Huang, S.-L., & Hsu, C.-J. (2015). A dual-factor model of loyalty to IT product: The case of smartphones. *International Journal of Information Management*, *35*(2), 215-228. https://doi.org/10.1016/j.ijinfomgt.2015.01.001

Lindell, M. K., & Whitney, D. J. (2001). Accounting for common method variance in cross-sectional research designs. *Journal of Applied psychology*, *86*(1), 114.

Liu, A., Urquía-Grande, E., López-Sánchez, P., & Rodríguez-López, A. (2022). How technology paradoxes and self-efficacy affect the resistance of facial recognition technology in online microfinance platforms: Evidence from China. *Technology in Society*, *70*, 102041. https://doi.org/10.1016/j.techsoc.2022.102041

Liu, T., Li, W., & Jia, X. (2023). Consumer data vulnerability, peer privacy concerns and continued usage intention of sharing accommodation platforms: The moderating roles of perceived benefits. *Information Technology & People*, *36*(6), 2234-2258. https://doi.org/10.1108/ITP-05-2021-0365

Liu, T., Yang, B., Geng, Y., & Du, S. (2021). Research on face recognition and privacy in China: Based on social cognition and cultural psychology. *Frontiers in Psychology*, *12*, 809736.

Lyu, T., Guo, Y., & Chen, H. (2024). Understanding people's intention to use facial recognition services: The roles of network externality and privacy cynicism. *Information Technology & People*, *37*(3), 1025-1051. https://doi.org/10.1108/ITP-10-2021-0817

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336-355. https://doi.org/10.1287/isre.1040.0032

Moriuchi, E. (2021). An empirical study of consumers' intention to use biometric facial recognition as a payment method. *Psychology & Marketing*, *38*(10), 1741-1765. https://doi.org/10.1002/mar.21495

Nan, D., Kim, Y., Huang, J., Jung, H. S., & Kim, J. H. (2022). Factors affecting intention of consumers in using face recognition payment in offline markets: An acceptance model for future payment service. *Frontiers in Psychology*, *13*, 830152. https://doi.org/10.3389/fpsyg.2022.830152

Nemati, H., Wall, J. D., & Chow, A. (2014). Privacy coping and information-sharing behaviors in social media: A comparison of Chinese and US users. *Journal of Global Information Technology Management*, *17*(4), 228-249. https://doi.org/10.1080/1097198X.2014.978622

Ogbanufe, O., & Gerhart, N. (2018). Watch it! Factors driving continued feature use of the smartwatch. *International Journal of Human–Computer Interaction*, *34*(11), 999-1014. https://doi.org/10.1080/10447318.2017.1404779

Owusu, A., Taana, I. H., Bakare, A. S., Abdurrahaman, D. T., & Broni Jr, F. E. (2020). Investigating the nexus between mobile apps adoption and privacy concerns among users: An empirical analysis from Ghana. *Technium Soc. Sci. J.*, *10*, 167.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, *88*(5), 879. https://doi.org/10.1037/0021-9010.88.5.879

Ramayah, T., Cheah, J., Chuah, F., Ting, H., & Memon, M. A. (2018). *Partial least squares structural equation modeling (PLS-SEM) using smartPLS 3.0: An updated guide and practical guide to statistical analysis*. Pearson.

Rasul, T., Wijeratne, A., Soleimani, S., & Lim, W. M. (2023). Where there’s sugar, there are sugar-related mobile apps. What factors motivate consumers’ continued use of m-Health? *Journal of Strategic Marketing*, *31*(4), 856-876. https://doi.org/10.1080/0965254X.2021.1999307

Ricardo, d. S. A., Moriguchi, S. N., & Andrade, D. F. (2016). Intention of adoption of mobile payment: An analysis in the light of the Unified Theory of Acceptance and Use of Technology (UTAUT). *RAI Revista de Administração e Inovação*, *13*(3), 221-230. https://doi.org/10.1016/j.rai.2016.06.003

Richardson, H. A., Simmering, M. J., & Sturman, M. C. (2009). A tale of three perspectives: Examining post hoc statistical techniques for detection and correction of common method variance. *Organizational Research Methods*, *12*(4), 762-800.

Shahzad, M. F., Xu, S., Lim, W. M., Hasnain, M. F., & Nusrat, S. (2024). Cryptocurrency awareness, acceptance, and adoption: the role of trust as a cornerstone. *Humanities and Social Sciences Communications*, *11*(1), 1-14. https://doi.org/10.1057/s41599-023-02528-7

Shang, D., & Wu, W. (2017). Understanding mobile shopping consumers' continuance intention. *Industrial Management & Data Systems*, *117*(1), 213-227. https://doi.org/10.1108/IMDS-02-2016-0052

Shmueli, G., Sarstedt, M., Hair, J. F., Cheah, J.-H., Ting, H., Vaithilingam, S., & Ringle, C. M. (2019). Predictive model assessment in PLS-SEM: guidelines for using PLSpredict. *European Journal of Marketing*, *53*(11), 2322-2347. https://doi.org/10.1108/EJM-02-2019-0189

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, 989-1015. https://doi.org/10.2307/41409970

Susanto, A., Chang, Y., & Ha, Y. (2016). Determinants of continuance intention to use the smartphone banking services: An extension to the expectation-confirmation model. *Industrial Management & Data Systems*, *116*(3), 508-525. https://doi.org/10.1108/IMDS-05-2015-0195

Tam, C., Santos, D., & Oliveira, T. (2020). Exploring the influential factors of continuance intention to use mobile Apps: Extending the expectation confirmation model. *Information Systems Frontiers*, *22*, 243-257. https://doi.org/10.1007/s10796-018-9864-5

Varian, H. R. (2009). Economic aspects of personal privacy. *Internet Policy and Economics: Challenges and Perspectives*, 101-109. https://doi.org/10.1007/b104899_7

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 425-478. https://doi.org/10.2307/30036540

Wang, L. (2024). *China Payment and Clearing Association: More than 80% of users use mobile payment every day*. WWW.XHBY.NET. Retrieved Jun 25 from https://www.xhby.net/content/s66225343e4b01424a8875497.html

Westbrook, R. A., & Oliver, R. L. (1991). The dimensionality of consumption emotion patterns and consumer satisfaction. *Journal of Consumer Research*, *18*(1), 84-91. https://doi.org/10.1086/209243

Wu, X., Zhou, Z., & Chen, S. (2024). A mixed-methods investigation of the factors affecting the use of facial recognition as a threatening AI application. *Internet Research*. https://doi.org/10.1108/INTR-11-2022-0894

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, *12*(12), 1. https://doi.org/10.17705/1jais.00281

Yan, Z., Yan, H., & Chen, Y. (2020). *Who's selling my face？*. Retrieved Oct from https://news.cctv.com/2020/07/14/ARTIIcp7s37vUIBn3Dx93WOO200714.shtml

Yeung, D., Balebako, R., Gaviria, C. I. G., & Chaykowsky, M. (2020). *Face recognition technologies: Designing systems that protect privacy and prevent bias*. Rand Corporation.

Yuan, S., Liu, Y., Yao, R., & Liu, J. (2016). An investigation of users' continuance intention towards mobile banking in China. *Information Development*, *32*(1), 20-34.

Zhang, W. K., & Kang, M. J. (2019). Factors affecting the use of facial-recognition payment: an example of Chinese consumers. *IEEE Access*, *7*, 154360-154374. https://doi.org/10.1109/ACCESS.2019.2927705

Zhong, Y., & Moon, H.-C. (2022). Investigating customer behavior of using contactless payment in China: A comparative study of facial recognition payment and mobile QR-code payment. *Sustainability*, *14*(12), 7150. https://doi.org/10.3390/su14127150