Investigation on users’ resistance intention to facial recognition payment: a perspective of privacy

Xusen Cheng1, Liyang Qiao1, Bo Yang1, Xiaoping Zhang1

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract

Despite the convenience of facial recognition payment (FRP), many consumers hesitate to use FRP. Drawing on the antecedent-privacy concern-outcome (APCO) macro model, this study investigates antecedents of privacy concerns and privacy fatigue in the context of FRP and how privacy concerns and privacy fatigue influence user’s resistance intention of FRP. A mixed-methods is used to address these issues. A semi-structured interview is first used to identify the antecedents of privacy concerns and privacy fatigue for facial privacy information. According to the research results, we develop research hypotheses and build the research model. By analyzing survey data from 394 respondents using Amos, this study finds that privacy experience, privacy control, privacy policy effectiveness, peer influence, and reputation significantly influence users’ privacy concerns for facial privacy information; in addition, privacy experience, privacy control, and negative media exposure significantly influence users’ privacy fatigue. Moreover, privacy concerns and privacy fatigue are significantly related to users’ resistance intention to FRP.

Keywords Facial recognition payment (FRP) · Privacy concerns · Privacy fatigue · APCO macro model · Users’ resistance intention to FRP

Bo Yang
yangbo@ruc.edu.cn
Xusen Cheng
xusen.cheng@ruc.edu.cn
Liyang Qiao
824953494@qq.com
Xiaoping Zhang
xiaoping_sdust@163.com

1 School of Information, Renmin University of China, 100872 Beijing, China

Published online: 05 November 2022
1 Introduction

With the rapid development of information technology, the payment methods are becoming increasingly diversified. Some new payment methods have emerged, such as fingerprint payment and facial recognition payment (FRP) [1]. Over past few years, FRP has become one of the most popular payment methods among Chinese people due to its convenience and efficiency [2]. Unlike other payment methods, people can complete payment only through facial recognition. Consumers can pay for products or services even if their phones are turned off. However, the number of FRP users is not as high as expected. Iimedia [3] reported that the number of FRP users was 61 million in 2018. This is partly because people may also be confronted with serious threats to their privacy facial information which service providers ask them to provide [4]. For instance, the BBC has reported that a law professor at Tsinghua University, resisted providing her facial privacy information for facial recognition, saying it would cause serious consequences if the information was leaked [5]. Additionally, Xinhua News Agency reported that some online black industry practitioners resold illegally obtained facial identity information and “photo activation” online tools on e-commerce platforms, which also brought trouble to the users of FRP [2]. Moreover, several cities, including San Francisco, Orlando and Somerville, have banned facial recognition technology to prevent misuse of personal facial information [3]. Privacy issues have been one of the biggest obstacles to the spread of FRP.

It is common that facial information is one of the most important biological information and is an important part of identity authentication [5]. When your facial information is accessed by other people or organizations, they can easily know your age [6], gender [7], and appearance. Since payment information is bound to facial information, the leakage of facial information may also lead to property loss. But when people are using FRP, the service provider can legally access and store the users’ facial privacy information for free [8]. Although some large FRP service providers have made a commitment to privacy protection, there were still some contingencies of information leakage caused by wrong operation or illegal operation [9]. As many people worry about privacy leaks, they may refuse to provide their facial information. Meanwhile, constantly being asked for access and dealing with privacy-related issues may make people feel exhausted and powerless because of the lack of proper management of their privacy information [10]. Therefore, they are more likely to refuse to use FRP to avoid being frequently asked for facial privacy information.

Against this background, a question needed to be explored is why consumers are reluctant to use FRP. Based on the existing literature, we identify two key factors to influence consumers’ intention to use FRP, privacy concerns and privacy fatigue [11]. Privacy concerns refer to people’s fear of the adverse consequences due to the misuse

---

1 BBC News. 2019. China facial recognition: Law professor sues wildlife park. https://www.bbc.com/news/world-asia-china-50324342.
2 Xinhua News Agency. 2020. Who’s selling our facial information? http://www.xinhuanet.com/politics/2020-07/13/c_1126232239.htm.
3 Consumer News & Business Channel (CNBC). 2019. San Francisco bans police use of face recognition technology. https://www.cnbc.com/2019/05/15/san-francisco-bans-police-use-of-face-recognition-technology.html.
Investigation on users’ resistance intention to facial recognition…

of their private information [9, 12]. It has been confirmed to affect consumers’ intention to disclose information across various contexts [13–15]. Additionally, privacy fatigue refers to the fact that consumers are bored and tired of privacy-related information [16], which is seen as an additional influential factor of the intention to use FRP. In the age of Internet, we often hear about privacy-related issues. The deluge of privacy issues in the news and frequent requests for privacy permissions can be annoying. Consequently, privacy fatigue may be an important factor influencing consumers’ intention to disclose facial information [10]. Although FRP has gained popularity in recent years, research on facial privacy in this context is still limited. Even though a recent study has explained the impact of privacy concerns and perceived risk on users’ resistance intention to FRP [2], we have no idea of domain-specific antecedents of privacy concern. To address the research gaps, this study employs antecedent-privacy concern-outcome (APCO) macro model [12] as the theoretical lens to investigate privacy concern and privacy fatigue in the context of FRP. Two research questions are as follows:

RQ1: What factors influence privacy fatigue and privacy concerns of user’s facial information?

RQ2: How do antecedents influence privacy fatigue and privacy concerns, and subsequently influence user’s response to facial recognition payment?

Our study is grounded on APCO model that indicates the relationship among antecedents, privacy concerns and users’ resistance intention [12]. A mixed-methods is used to answer the above research questions [17, 18]. To answers RQ1, we conduct a qualitative study to explore the antecedents of facial privacy concerns and privacy fatigue in the FRP setting and then build our research model. To answer RQ2, we conduct a quantitative study to empirically test research hypotheses.

This study makes theoretical contributions to the research on facial information privacy. First, our work enriches existing studies on privacy issues by identifying domain-specific antecedents of privacy concerns and privacy fatigue in the context of FRP from three levels, i.e., society, individual and organization level. Second, this study extends APCO model to the context of FRP and adding privacy fatigue to the APCO macro model. Third, a mixed-methods is used in this study, which offers a new insight for future empirical research.

The rest of this study is organized as follows. First, we discuss the literature review on FRP, information privacy and APCO model. Then we present our research methods, data analysis and results analysis. Finally, this study is concluded with theoretical and practical implications, limitations, and suggestions for future directions.

2 Literature Review

The literature review is divided into three parts. The first part will discuss the research related to facial recognition and FRP. The second part will define facial information privacy and review related works about information privacy. In the third part, we employ APCO model as the foundation of the research framework to explain the relationship among antecedents, facial privacy concerns, privacy fatigue and users’ resistance intention.
2.1 Facial recognition and FRP

Facial recognition technology has a long history. Galton [19] initially proposed that facial information could be used for personal identification [20]. In the last 30 years, research into automatic facial recognition technology has reached a climax. With the rapid development of facial recognition technology, it is increasingly used in the payment industry, and this phenomenon has attracted considerable attention from academic researchers. For instance, Morosan focused on hotel facial recognition systems and found that performance expectancy, trust in organization, and positive anticipated emotions influenced users’ intentions [21]. Gao developed econometric models to analysis usage of FRP, and found that the social presence and herd effect have a significant influence on consumers’ usage intention to FRP [22]. Moriuchi conducted an empirical study and found that consumers would rather use a biometric payment system in stores than online and self-efficacy has a moderating effect on users’ willingness to use [23]. Ciftci focused on costumers’ usage intention at quick-service restaurants and indicated that perceived performance expectancy, social influence, and trust in the system significantly and positively affect customer usage intention to FRP based on the unified theory of acceptance and use of technology (UTAUT) [24].

Existing studies advance our knowledge concerning FRP usage intention. However, research on why people resist to use FRP from the perspective of privacy concern is rather limited. Some studies just pointed out that FRP technology is at risk of revealing personal facial information, and raised questions about the protection of personal facial information [25]. As a result, people tend to refuse to use FRP. So, this study focuses on users’ resistance intention to FRP from the perspective of privacy protection.

2.2 Information privacy

Information privacy attracted increasing attentions from scholars [12, 26–28]. In the field of e-commerce, information privacy has become a hot topic. In the research about share-economy, Ursin focused on information privacy protection in data sharing time [29]. When it comes to e-government, Agozie investigated the relationship between privacy information transparency and privacy fatigue, and found that privacy information transparency has significant positive effect on both cynicism behavior and emotional exhaustion [30]. In the context of social media, James examined individuals’ perceptions of the risk which their online social networks activity caused to others’ information [31]. Yu found perceived risk and privacy concerns can influence people’s information disclosure intention based on Elaboration Likelihood Model (ELM) [32].

Privacy issues have become more prominent in the Internet age. Various private information like payment information, location information and facial information may be destroyed. Cellary explained why the methods that Visible Internet accepted to protect payment information privacy cannot be applied to Unseen Internet, and showed directions of possible solutions [33]. Krishen conducted a mixed-methods study to explore users’ perceived fairness to location information privacy when they use location-based services. And the study indicated that with higher internal locus
of control, higher attitude toward the communication, and lower level of privacy concern, people will pay more attention to the fairness perceptions of privacy-related policies [34]. Xu extended the privacy calculus model and investigated the influence of compensation, industry self-regulation, and government regulation on individual privacy decision making in location-based services [35].

Privacy concerns have been proved to have a significant impact on people’s willingness and behavior such as reducing information disclosure or resistance [9, 10, 12]. Studies have shown that privacy concerns lead people to take a series of protective measures to deal with the possible consequences of privacy problems, for example, they may sue the company to protect their personal information, make negative comments on the company, or even refuse to use the service [13, 14, 36]. Privacy fatigue has the impact on user behavior through different ways. Frequent requests for privacy information and permissions can lead to weariness and exhaustion [10]. Unlike privacy concerns, studies have shown that fatigue prompts users to react negatively to privacy issues or cut off the service for staying away from privacy issues [37]. Therefore, a combination of privacy concerns and privacy fatigue may be the reason why individuals refuse to use services that require private information. It can be observed that most previous studies pay attentions to privacy information like ID number, home address, bank account, etc. The unique features of facial information may challenge these results from different contexts. In addition, the antecedents of both privacy concerns and privacy fatigue need to be explored further.

2.3 APCO macro model

The antecedent-privacy concern-outcome (APCO) macro model proposed by Smith provides a theoretical framework to explain the relationship between antecedents of privacy concerns, privacy concerns and outcome of privacy concerns [12]. In this model, antecedents of privacy concerns include privacy experience, privacy awareness, personality differences, demographic differences and culture/climate. And outcomes contain behavior, trust, regulation, risks/costs. This model is a mix of various disciplines [13], such as information system [14], human behavior [38, 39], marketing [40, 41]. Dienv improved the APCO model by adding level of effort, peripheral cues, biases, heuristics, misattribution to the influence on privacy calculus and behavioral reactions [42].

APCO model has been widely used in different research contexts to investigate privacy concern, such as social media and sharing-economy [12]. For example, Lakton investigated information privacy in social networks and found that privacy experience and gender have a significant influence on privacy concerns and privacy concerns, risk, benefit and enjoyment can affect users’ continuance intention [43]. Li employed APCO model to study information privacy in electric scooter sharing platforms and indicated that privacy experience, privacy awareness, usage regularity and geographic regularity can affect users’ privacy concerns for payment information and location information, and users’ privacy concerns finally have a positive effect on users’ information privacy protective response [13].
The mixed-methods combines qualitative study and quantitative study, and can be used to investigate some phenomenon that qualitative or quantitative study alone can’t completely, reasonably, comprehensively explains [11, 17, 18, 44, 45]. The mixed-methods has the advantages of both qualitative and quantitative, and can provide richer and more reliable conclusions. [46]. Therefore, we employed a mixed-methods to explore facial information privacy in the FRP context. The qualitative study consists of interview, coding and results analysis, while the quantitative study tests the assumptions and model generated by qualitative analysis results [47]. Based on previous studies with mixed-methods, the process of this approach is shown in Fig. 1.

3.1 Qualitative study

Qualitative study in our approach aims to deeply explore the antecedents of facial privacy concerns and privacy fatigue for modeling.

3.1.1 Data collection

The semi-structured interview method is used to collect data. Two researchers interviewed our participants. Each interview data was taped and converted into a transcript [48]. The interview of this approach is divided into three parts. In the first part, the interviewees introduce their basic information, including age, educational background and experience of using FRP. In the second part, the interviewees were asked about the factors influencing their facial privacy concerns and privacy fatigue. In the third part, we ask questions based on participants’ answers to supplement the interview materials [49].

We took a random sample of people who had used FRP. In order to ensure that the interview data is accurate, we asked them about their FRP experience during the interview. We transcribed each interview in real time and every interview was anonymous to avoid potential informant bias. Besides, according to Eisenhardt [50], all of
researchers have been trained to react to responses for avoiding giving guidance to interviewees. In the end, we collected 22 interview data in total which was encoded A1-A22. Among them, there are 14 female respondents and 8 male respondents, and most of them are aged between 20 and 30 with a bachelor’s degree or above.

### 3.1.2 Qualitative data analysis and results

First, we summarized the collected interview data into interview documents [51] And then, we analyze the interview documents by Grounded theory three-stage coding [52]: open coding, axial coding, selective coding. We complete the data coding as shown below:

1. **Open coding**: In this process, we extracted all the phrases about facial information privacy concerns and privacy fatigue, divided them into meaningful segments, and conceptually classified, compared and marked them.
2. **Axial coding**: Firstly, we sorted through the documents and examined the relationship between each category and phenomena. Secondly, we examined whether the actual studies support this hypothetical relationship. Finally, we organized the initial concepts into higher-order categories [51].
3. **Selective coding**: We developed a clear story line at a conceptual level and tried to explain the initial results with APCO model. The quantitative study will be used to further analyze the qualitative results.

We show the results of our analysis in Tables 1 and 2, where all of the representative quotations were mentioned by multiple people. The data analysis process identified seven antecedents of facial privacy concerns: privacy experience, privacy awareness, privacy control, privacy policy effectiveness, reputation, peer influence, and negative media exposure. And it also identified four antecedents of privacy fatigue: privacy experience, privacy awareness, privacy control, and negative media exposure.

Privacy experience means that when a person has been subjected to privacy invasion or related experiences, his perception of facial information privacy will be more sensitive and he will be more concerned about facial privacy leakage [53, 54]. However, the tedious experience of dealing with privacy issues can make people feel tired and reduce the desire to deal with them again [55]. Privacy awareness means one has the knowledge of privacy issues, privacy protection and the organization’s privacy practices [56]. Those with the relevant knowledge are better able to understand the consequences of disclosing their privacy than those who do not. At the same time, constant attention to facial privacy can cause them to worry more. If they don’t understand the organization’s privacy practices, they will feel helpless when faced with privacy issues. The third one is privacy control, meaning the degree of people’s willing to have access to their private information [57]. When they don’t know what’s going on with their facial information, they show concern about this. The service providers’ reputation also affects people’s attitude. Specifically, people will choose the organization which has better reputation [54]. People in society are also influenced by those around them, we call this phenomenon peer influence [58]. Negative media exposure means news media coverage of a privacy breach, or criticism of a service provider. And it can heighten people’s facial privacy concerns [59] and encourage privacy fatigue. Therefore, we selected privacy experience, privacy awareness,
privacy control, privacy policy effectiveness, reputation, negative media exposure and peer influence as the antecedents of privacy concerns. And privacy experience, privacy awareness, privacy control and negative media exposure influence privacy fatigue. Besides, we divided seven antecedents into three levels: social level, organization level and individual level and the research model is shown in Fig. 2.
3.2 Quantitative study

3.2.1 Hypotheses development

Based on the results of qualitative study, we conducted a quantitative study on the relationship among antecedents, facial privacy concerns, privacy fatigue, and users’ resistance intention to use FRP.
People who have been the victim of privacy invasion may have stronger concerns when it comes to facial information privacy [9]. In other words, the privacy experience influences consumers’ attention to facial privacy issues and those who have not experienced a privacy invasion are not be aware that it may happen to them [60]. Previous studies have shown that accumulated privacy experience and negative emotion can lead to increase the level of privacy concerns, and then increased resistance intention [61]. In the context of FRP, users were asked to provide their facial information. For people who have already experienced privacy invasion, they will consider whether providing facial information will make them the victim of another facial privacy violation, so they act more concerned than others. However, people who have experienced privacy problems or failed to deal with privacy issues may choose to stay away from what’s bothering them. The following hypotheses are proposed:

H1a. Privacy experience has a positive effect on privacy concerns for facial information.

H1b. Privacy experience has a positive effect on privacy fatigue.

Privacy awareness means having the knowledge of privacy issues and an organization’s privacy measures and practices [12]. People with a high level of privacy awareness can clearly understand the importance of personal facial information and the consequences of privacy leakage, so they will have a stronger concern about facial information. For example, consumers who are unaware of name removal operations tend to be less concerned about privacy than those who have a strong awareness of their privacy [62, 63]. People know that facial information is tied to their payment information and identity information, so they are more careful about giving facial information. Similarly, if there is a lack of knowledge about privacy, you will feel powerless when faced with privacy issues. We therefore state the following hypotheses:

H2a. Privacy awareness has a positive effect on privacy concerns for facial information.

H2b. Privacy awareness has an opposite effect on privacy fatigue.

The control of personal information privacy is a method of privacy protection, and privacy control reflects people’s desire to control private information like knowing how facial information is being collected and processed. In the context of FRP, privacy controls mean that users want to know how information about their facial information is being collected [64], used and shared. Studies have shown that many people want to control their own private information, which also reflects their concern about private information [57, 65–67] In addition, long periods of attention and dealing with privacy-related issues can cause fatigue, and high levels of privacy control are more likely to cause privacy fatigue. So, we assert:

H3a: Privacy control has a positive effect on privacy concerns for facial information.

H3b: Privacy control has a positive effect on privacy fatigue.

Privacy policy effectiveness is defined by FTC’s Fair Information Practice Principles (FIPPs) focusing on core privacy principles [68]. And FIPPs divided privacy policy to five dimensions: notice, choice, access, security, and enforcement [69]. Notice is that an organization needs to publicly state its privacy policy before collecting personal information [70]. And choice refers to providing users with a choice after informing them what personal information they will collect and how they will
use it. Access means that the privacy policy should allow users to access their stored personal information for the purpose of checking its completeness and accuracy.\[71]\). Security is that privacy policies should reflect the protection of information, and enforcement is the need for organizations to strictly enforce their privacy policies\[69]\). Previous studies have shown that privacy policies are important to users’ privacy decisions, and that effective privacy policies can help reduce users’ privacy concerns\[72, 73]\], and in this study we will classify policy effectiveness as an antecedent at the organizational level. The following hypotheses is proposed:

H4: Privacy policy effectiveness has an opposite effect on privacy concerns for facial information.

The reputation of the service provider is an indicator of the comprehensive service provider’s ability, scale, behavior, product and service expertise, social characters, attitude towards customers, communication ability, etc.\[74]\). What the users are concerned about is how the FRP service providers deal with their privacy information, and they take the providers’ scale and ability as the guarantee, and the attitude of the service providers as the dependence\[75]\). According to the previous studies, providers’ reputation can directly influence users’ privacy concerns and indirectly influence users’ attitudes through trust\[54, 76]\). We also use it as an antecedent at the organizational level. So, we state the following hypothesis:

H5: Reputation has an opposite effect on privacy concerns for facial information.

Peer influence refers to the impact of privacy concerns of people around or peers on a target user. We study it at the social level, because peer influence involves social communication, social influence and herd psychology\[58, 77]\). Peer influence can be either positive or negative for privacy concerns. For example, people may reduce their concerns about facial privacy because people around them do not pay attention to privacy issues, or they may become worried because of the concerns of people around them\[78]\). According to our qualitative study, majority of interviewees expressed concerns about privacy and also said they would be more concerned due to their peers’ concerns. Therefore, in this study, peer influence refers to the impact of peer privacy concerns on target users’ emotions. According to the previous studies, the temporal organization of people’s behavior on social platforms is influenced by the behavior of their peers\[79]\), friends who have already made a purchase also increase people’s pressure to make a purchase\[80]\). Therefore, we state the following hypothesis:

H6: Peer influence has a positive effect on privacy concerns for facial information.

Negative reports and social news about the service providers will lower people’s impression of the service providers, which will lead to the associated negative news when using FRP\[59]\). Besides, negative media exposure can also make users feel like the facial information privacy invasion is happening to them. In recent years, more and more people are paying attention to privacy issues, which means that negative news reports about privacy issues will attract a lot of eyes. For example, companies such as Apple and Facebook have received criticism and complaints in recent years for mishandling customer information\[81, 82]\), and these can lead to distrust and worry. Similarly, the deluge of negative media exposure about privacy has created not just anxiety, but boredom. Some respondents mentioned that they now skip news about privacy. The following hypotheses is proposed:
H7a: Negative media exposure has a positive effect on privacy concerns for facial information.
H7b: Negative media exposure has a positive effect on privacy fatigue.

Smith explains and measures privacy concerns from seven perspectives [9]: collection, unauthorized secondary use (internal), unauthorized secondary use (external), improper access, errors, reduced judgment, combining data. In the context of FRP, collection means users worry about their facial information being collected and stored by service providers [83]. Unauthorized secondary use represents unauthorized use of facial information for another purpose, either within or outside the organization [83]. Improper access means that facial information is easily viewed and accessed by someone else who is not authorized to do so and errors is the loss or disclosure of facial information due to improper operation or error [9]. Because of the fear of this happening, users will be less willing to pay with their faces. Numerous studies have demonstrated the impact of privacy concerns on users’ behavior and intentions [60, 84]. The latest research shows privacy concerns’ influence in marketing consumer research [85, 86], app uses [87], medical treatment and health [88], and e-government [89].

It’s not just privacy concerns, but weariness and fatigue over privacy issues that have an impact on users’ attitudes. For example, users can become tired or even resistant when they are frequently exposed to privacy issues or asked for privacy rights [10]. We think of the powerlessness and boredom that comes with privacy fatigue [15, 16]. Once efforts to solve privacy issues fail to achieve the desired results, users will also generate a mismatch between the benefits and efforts, resulting in privacy issues fatigue and disengagement [90, 91]. On the other hand, in the face of demands for privacy and the possible consequences of privacy disclosure, fatigue makes people want to get rid of privacy and cut off services [92]. For instance, respondent A21 mentioned “I don’t want to see privacy related topics anymore, and I don’t want to read the privacy statement contract provided by the app. When I encounter those, I usually just quit (the app)”. Similarly, respondent A3 also mentioned that he felt tired when the facial payment app tried to obtain his facial information through the microphone and camera. Some users who suffer from privacy fatigue will choose to stay away from services requiring information privacy rather than compromise and cynicism due to low sunk costs of abandon [15, 93]. So, when users have a high level of privacy fatigue, they have enough reason to choose not to use the FRP. Therefore, we state the following hypotheses:

H8: Privacy concerns for facial information have a positive effect on users’ resistance intention.
H9: Privacy fatigue has a positive effect on users’ resistance intention.

Our hypotheses are shown in Fig. 3.

3.2.2 Data collection

We distributed online questionnaires by wjx.com, which is an extremely popular data collection platform in China. Before the questionnaires were sent out, 11 randomly selected volunteers were invited to fill in the questionnaire. According to the results, they all took more than 74s to answer the questionnaire, so the results from
participants whose answer time was less than 60s would be excluded. We applied random sampling and collected 588 pieces of data from July 20 to July 31. Among these responses, 194 were excluded because of multiple repeated selection or short response time. We finally got 394 pieces of valid data, and the response rate of the online survey is 67.0% (>50%), which is acceptable [94].

This online survey was conducted in China, so we first translated all the original items from English into Chinese. In order to ensure the accuracy of the questions, we invited 12 users with experience of FRP to check whether the questionnaire items can be understood. Next, we made some modifications to the questionnaire items according to their suggestions. Finally, we re-translated the Chinese questionnaire into English to determine the consistency of the two versions.

3.2.3 Measures

We conduct an online survey to verify our hypotheses. We measure most constructs using existing scales. Privacy experience was measured using two items from Yuan [54]. And we measured privacy awareness using two items from Xu [35]. We measured privacy control using three items from Malhotra [64] and privacy policy effectiveness using two items from Chang [69]. Negative media exposure is measured by two items from Cheng [11]. FRP service providers’ reputation is measured by two items from Yuan [54]. We adapted three items from Xu [35] to measure facial privacy concerns. Privacy fatigue was measured using two items from Choi [10], and resistance intention was measured by three items from Mittelstaedt [95]. Since few studies focused on the impact of peer influence on privacy attitudes, the scale of peer influence is designed by ourselves. We used five-points Likert scales ranging from 1 (strongly disagree) to 5 (strongly agree) in each scale. All items are presented in Appendix 1.
3.2.4 Sample characteristics

Of the 394 respondents, 52.3% were male and 47.97% were female, and the gender ratio is relatively balanced. Most respondents were aged 20–40 years. Those with a bachelor’s degree were in the majority, accounting for 77.67%. The demographics of respondents are shown in Table 3.

4 Quantitative data analysis and results

In this section, measurement model and structural model will be performed. Structural Equation Modeling (SEM) using maximum likelihood estimation was applied to explore the hypothesized research model. And SEM was considered as an appropriate method for investigating the hypothesized relations between multiple independent and dependent variables. In specific, this study focused on APCO model and tried to explain the relationships between various variables, which is suitable for covariance-based (CB) SEM [96]. So, we used CB-SEM via SPSS and Amos 24 to conduct a statistical analysis. In addition, the sample size collected in this study also meets the requirements of CB-SEM (>200) [97]. Before the analysis, we examined the normality of the data distribution. All items’ skewness and kurtosis values (shown in Table 4) are less than 3. Q-Q plots are satisfactory and Shapiro-Wilk test results also meet the criteria of significance, indicating that data is almost normally distributed [98, 99]. It suggests that the data is suitable for Amos analysis.

4.1 Exploratory factor analysis

Before conducting exploratory factor analysis, we used Kaiser-Meyer-Olkin (KMO) measure and Bartlett’s test of sphericity for sampling adequacy. According to the results, KMO measure of sampling adequacy is 0.846(>0.6) and the significance
Bartlett’s test of sphericity is 0.000, which indicates well suited to factor analysis [100, 101]. We conducted exploratory factor analysis on 23 items and extracted 7 principal factors which could basically reflect these 23 items. Additionally, these 7 factors can explain 75.04% of the variance. The results of exploratory factor analysis show that all items are bearing the corresponding factors and consequently reflects the discriminant and convergent validity [57].

4.2 Measurement model

First, measurement model is tested. The results of the reliability and convergent validity of model are shown in Table 4. The results show that the values of Cronbach’s alpha and composite reliability (CR) of all constructs exceed 0.7, indicating the reliability of the model is acceptable [102]. Loadings of factors corresponding to corresponding constructs are above 0.7 and the average variance extracted (AVE) is above 0.5, indicating that convergence validity is satisfied [102]. Table 5 shows the result of discriminant validity and the correlation coefficient between each variable. According to the result, the square roots of all AVE on the diagonal are greater than the correlation coefficients between all constructs [103], suggesting the discriminant validity is satisfied.

4.3 Structure model

The estimated results are shown in Fig. 4. The results showed that privacy experience was significantly related to privacy worry and privacy fatigue, and thus H1a
and H1b were accepted. Privacy awareness was not significantly related to facial privacy concerns and privacy fatigue, and thus H2a and H2b were rejected. Privacy control had a significant influence on facial privacy concerns and privacy fatigue, thus H3a and H3b were accepted. Privacy policy effectiveness was negatively related to facial privacy concerns, supporting H4. The reputation of the service provider had

Table 5 Discriminant validity

|     | NME  | PI    | PA    | PCON  | PC    | PE    | PF    | PPE   | RI    | RE    |
|-----|------|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| NME | 0.938|       |       |       |       |       |       |       |       |       |
| PI  | 0.423| 0.811 |       |       |       |       |       |       |       |       |
| PA  | 0.418| 0.468 | 0.812 |       |       |       |       |       |       |       |
| PCON| 0.396| 0.539 | 0.535 | 0.889 |       |       |       |       |       |       |
| PC  | 0.321| 0.389 | 0.681 | 0.610 | 0.794 |       |       |       |       |       |
| PE  | 0.386| 0.367 | 0.553 | 0.600 | 0.500 | 0.828 |       |       |       |       |
| PF  | 0.325| 0.265 | 0.406 | 0.380 | 0.431 | 0.473 | 0.782 |       |       |       |
| PPE | -0.140| -0.119 | -0.172 | -0.354 | -0.165 | -0.406 |       | -0.179 | 0.891 |       |
| RI  | 0.273| 0.330 | 0.360 | 0.586 | 0.404 | 0.409 | 0.421 | -0.218 | 0.823 |       |
| RE  | -0.139| -0.180 | -0.106 | -0.186 | -0.098 | -0.337 |       | 0.593 | 0.929 |       |

The indicators of model fit are shown in Table 6. According to the results, the values of indicators of measurement model meet the recommended values (CFI=0.947>0.9, TLI=0.945>0.9, NFI=0.906>0.9, IFI=0.948>0.9, GFI=0.901>0.9, RMSEA=0.054<0.08, SRMR=0.0689<0.08, χ²/df=2.14) [70, 104, 105]

Table 6 Model fit

| Indicator | Value | Standard |
|-----------|-------|----------|
| CFI       | 0.947 | >0.9     |
| GFI       | 0.901 | >0.9     |
| NFI       | 0.906 | >0.9     |
| IFI       | 0.948 | >0.9     |
| TLI       | 0.935 | >0.9     |
| RMSEA     | 0.054 | <0.08    |
| SRMR      | 0.0689| <0.08    |

Table 7 Effect overview

| Effect     | Standardized weight | p value | Result          |     |
|------------|---------------------|---------|-----------------|-----|
| PE→PCON    | 0.270               | 0.00    | Supported       |     |
| PA→PCON    | -0.035              | 0.647   | Rejected        |     |
| PC→PCON    | 0.341               | 0.00    | Supported       |     |
| PPE→PCON   | -0.228              | 0.00    | Supported       |     |
| RE→PCON    | 0.131               | 0.012   | Reversely support |     |
| PI→PCON    | 0.296               | 0.00    | Supported       |     |
| NME→PCON   | 0.058               | 0.209   | Rejected        |     |
| PE→PF      | 0.292               | 0.00    | Supported       |     |
| PA→PF      | 0.047               | 0.637   | Rejected        |     |
| PC→PF      | 0.213               | 0.023   | Supported       |     |
| NME→PF     | 0.125               | 0.044   | Supported       |     |
| PCON→RI    | 0.498               | 0.00    | Supported       |     |
| PF→RI      | 0.232               | 0.00    | Supported       |     |
Investigation on users’ resistance intention to facial recognition…

Investigation on users’ resistance intention to facial recognition…

a positive effect on the facial privacy concerns, and thus H5 was reversely supported. Peer influence had a positive effect on privacy concerns, and thus H6 was supported. Negative news coverage had no significant impact on privacy concerns but had a significantly positive influence on privacy fatigue, and thus H7a was accepted and H7b was rejected. Both facial privacy concerns and privacy fatigue had a positive influence on resistance intention, and thus H8 and H9 were accepted. According to the result, 29% of the variance in privacy fatigue, 59% of the variance in privacy concerns for facial information, and 40.4% of the variance in users’ resistance intention can be explained by exogenous variables. And the percentages of variances were above 0.10, which suggested a satisfactory model [106].

5 Discussion and conclusion

In this section, we will summarize the findings of the research, and present the theoretical and practical implications of this paper. Finally, we will conclude the deficiencies and prospects of this study.

5.1 Research findings

First, to answer of RQ1 “What factors influence privacy fatigue and privacy concerns of user’s facial information?”, we conducted a semi-structured interview. We found seven antecedents which cause users’ privacy concerns for facial information in the context of FRP. Among them, we divided privacy experience, privacy awareness and privacy control into individual level antecedents. Privacy policy effectiveness and service providers’ reputation are at the organizational level. Peer influence and negative media exposure belong to the social level. At the same time, we have discovered four antecedents of privacy fatigue: privacy experience, privacy awareness, privacy
control and negative media exposure. Based on the results of the qualitative analysis, we developed 13 hypotheses and established the research model.

Second, to answer RQ2 “How do antecedents influence privacy fatigue and privacy concerns, and subsequently influence user’s response to facial recognition payment?”. We developed a research model based on APCO model and the results of qualitative study. Research results showed that privacy concerns for facial information and privacy fatigue have a significant positive effect on users’ resistance intentions. And each antecedent has a different impact on privacy concerns and privacy fatigue. According to the results, privacy experience, privacy control, reputation and peer influence have a positive effect on users’ privacy concerns for facial information and privacy policy effectiveness has a opposite effect on users’ privacy concerns. In addition, privacy experience, privacy control and negative media exposure have a positive effect on users’ privacy fatigue.

Third, according to research results, privacy awareness has no significant impact on privacy concern for facial information and privacy fatigue. A plausible explanation is that individuals who are aware of privacy issues are more likely to find a way to protect their private information from risks and threats [107]. As a result, they don’t get too worried or tired about facial information privacy issues [108, 109]. Besides, contrary to our hypothesis, service providers’ reputation negatively influences privacy concerns. The major FRP service providers in China are large enterprises dominated by Alibaba and Tencent. It is no exaggeration to say that they hold the private information of almost all Internet users in China. From the consumer point of view, these two companies have the power and incentive to sell consumers’ personal data for financial gain, which are more likely cause social panic and consumer concerns. Negative media exposure also has no significant impact on privacy concerns for facial information. One possible explanation is that people are so skeptical about the authenticity of media exposure that they don’t empathize with events. As a result, some news reports that may appear false to consumers are not enough to cause their concern their facial information privacy. Moreover, individuals who are tired of privacy issues may experience feelings of boredom rather than empathy in response to negative media exposure.

5.2 Theoretical implications

The findings of this study provide several theoretical contributions. First, previous studies have focused on location privacy in sharing transportation and property privacy in payments. Compared with them [10, 13, 14], this study expanded the research range and took facial information privacy as the research object, so as to prepare for future research on facial information privacy. In this study, facial privacy information is proposed and empirical research is carried out, and we hope that it can receive the same attention as payment information and location information, which contributes to existing studies on privacy issues. Besides, this study addresses this research gap by developing a theoretical model to investigating the relationships between antecedents, privacy concern, privacy fatigue and users’ response to FRP.

Second, we employed APCO model into the study of facial information privacy. Based on previous studies [11, 14, 44] that raised the APCO model or used it to
investigated privacy issues in social media or location-based service, we extended the application of APCO macro model to FRP context and conducted an empirical study to prove the effectiveness of APCO model in the FRP context. This study finds several domain-specific antecedents of privacy concerns and privacy fatigue in the e-payment context. Compared with previous studies based solely on individual reasons [9, 12, 42], this study measures the influence of antecedents from individual level, organization level and society level so that we can understand more comprehensively how privacy concerns and privacy fatigue develop. Meanwhile, privacy concerns and privacy fatigue have some common antecedents, and both of them at a high degree will lead to users’ resistance intention, so it is necessary to add privacy fatigue into the APCO model to better explain its impact on users’ behavior. The influence of privacy fatigue is also significant in many contexts, and we believe that the modified APCO model can more effectively explain the influence of antecedents on individuals’ intention and behavior [10, 30]. Therefore, this study contributed to the literature of APCO and expanded the application scenarios of APCO model.

Third, we conducted a mixed-methods study. Few previous studies have focused on antecedents of privacy concerns in the FRP context. As far as we know, Liu et al. adopted an online survey to investigate users’ resistance intention on FRP by integrating the factors in privacy calculus theory [2]. However, this study only examines antecedents that are frequently verified in various context, and several domain-specific antecedents of FRP are not been found. So, we identify key antecedents by conducting semi-structured interview, which is suitable for exploring novel and theoretical underpinning fields [17, 18, 44, 46]. And based on the results of qualitative analysis, we obtained the antecedents confirmed in previous studies, and also identified several new antecedents such as peer influence and reputation.

5.3 Practical implications

Our study has some practical implications. According to our research, concerns and fatigue about facial privacy can lead users to resist facial recognition payments, and we explore the antecedents from the perspectives of individuals, organizations, and societies, providing a reference for FRP service providers, and news media. First, for the individual level, privacy control plays a significant role in the influence of privacy concerns and privacy fatigue. In order to avoid users’ anxiety and fatigue about facial privacy, service providers should provide better channels to satisfy users’ desire to control facial privacy and let users feel that they can master the storage and use of personal facial information. For example, service providers should give users the right to access their historical operation of facial information in the system. In addition, the service provider should not only have the right to access user facial information, but also undertake the obligation to protect users’ privacy, upgrade and improve the risk control system, and promise not to conduct unauthorized operations, and should conduct regular security checks on the database system to avoid unauthorized third-party operations that may bring bad privacy experiences to users.

Second, for the organization level, it is necessary for service providers to ensure the effectiveness and completeness of privacy policies because the effectiveness of privacy policies has a significant impact on users’ privacy concerns. On the one hand,
service providers need to make privacy policies easy to understand, rather than putting users to sleep with lengthy statements. In order to make users better understand the privacy policy of FRP, service providers can extract key points in the privacy policy as a short privacy statement. Users can choose to view a short or full privacy policy on the FRP app. And on the other hand, FRP service providers need to have complete privacy provisions and make sure they are implemented effectively so that users feel secure about providing their facial information. Moreover, setting a channel to communicate with users for get feedback and improve privacy policy according to their suggestions is vital for the platform.

Third, for the social level, peer influence can also exacerbate privacy concerns, and negative exposure of privacy issues can make people tired and resistant based on the research findings. The news media should choose the key privacy issues to report, and should not attract users’ attention by exaggeration or intimidation, so as to avoid excessive anxiety and resistance. Media are suggested to set up a column on privacy issues, so that users in need can browse relevant news. Moreover, it is necessary to report negative news with specific preventive measures, and provide suggestions for individuals to adopt. When the concerns and fatigue of facial privacy information in the society are gradually reduced and people’s facial information can be reasonably protected, FRP can be better promoted and give full play to its advantages. This research on users’ resistance intentions also gives them an inspiration on how to promote FRP. In addition, this research could provide many business and social implications regarding the privacy behavior part of users’ facial recognition payment which could be encouraged to increasing in the COVID-19 influenced period to help protect health and safety.

5.4 Limitations and future research

Our study has several limitations. Firstly, the antecedents of privacy concerns and privacy fatigue are limited in the context of FRP, and may not be able to be generalized to other contexts. So, future study could investigate users’ behavior in other payment environment. Secondly, this study was conducted in China, and the respondents were limited to Chinese FRP users, so the results may not be valid in other cultural contexts. Future study could conduct surveys in different regions or countries.

6 Appendix 1: Measurement scales

| Construct              | Item | Content                                                                 | Resource |
|------------------------|------|-------------------------------------------------------------------------|----------|
| Privacy experience     | PE1  | I was a victim of facial privacy invasion.                               | [54]     |
|                        | PE2  | I believe that my facial privacy was invaded by other people or organizations. |          |
| Privacy awareness      | PA1  | I am aware of the privacy issues and practices in FRP.                   | [35]     |
|                        | PA2  | I follow news and developments about privacy issues and privacy violations regarding FRP. |          |
| Construct                      | Item | Content                                                                 | Resource |
|-------------------------------|------|-------------------------------------------------------------------------|----------|
| Privacy control               | PC1  | My control of personal facial information lies at the heart of facial privacy. | [64]     |
|                               | PC2  | I believed that facial privacy is invaded when control is lost or unwillingly reduced as a result of FRP. |          |
| Privacy policy effectiveness  | PPE1 | With the privacy policy, I believe that my facial information will be kept private and confidential by service providers. | [69]     |
|                               | PPE2 | I believe that the privacy policy posted by service providers are an effective way to demonstrate their commitments to privacy. |          |
| Reputation                    | RE1  | This service provider of FRP has a good reputation.                     | [54]     |
|                               | RE2  | This service provider of FRP has a reputation for offering good products or services. |          |
| Peer influence                | PI1  | I feel like people around me are worried about facial information disclosure and infringement in FRP. | Self-developed |
|                               | PI2  | People around me remind me to protect my facial information from being leaked or infringed. |          |
|                               | PI3  | People around me pay attention to the protection of their facial information. |          |
| Negative media exposure       | NME1 | I often heard or read about the negative news of the company who provides FRP services during the last year. | [11]     |
|                               | NME2 | I often heard or read about the negative news about facial information disclosure during the last year. |          |
| Privacy concerns              | PCON1| I am concerned about providing my facial information because it could be leaked and used in a way I did not foresee. | [35]     |
|                               | PCON2| I am concerned about my facial information that is recorded on FRP because it could be used to identify me. |          |
|                               | PCON3| I am concerned that unauthorized parties could use my facial information to impersonate me. |          |
| Privacy fatigue               | PF1  | I am tired of facial privacy issues.                                     | [10]     |
|                               | PF2  | It is tiresome for me to care about facial privacy.                      |          |
| Resistance intention          | R11  | I will try NOT to use FRP.                                               | [95]     |
|                               | R12  | I will NOT use FRP in the future.                                       |          |
|                               | R13  | I will NOT use FRP if I have alternatives.                               |          |

**Acknowledgements** We would like to thank National Natural Science Foundation of China(Grant No. 72061147005) and fund for building world-class universities (disciplines) of Renmin University of China (Project No. KYGJA2022002) for providing funding for part of this research. We also thank the Metaverse Research Center of Renmin University of China.

**Declarations**

**Datasets** The data that support the findings of this study are available from the corresponding author upon request.
References

1. Zhong, Y., Oh, S., & Moon, H. C. (2021). Service transformation under industry 4.0: Investigating acceptance of facial recognition payment through an extended technology acceptance model. *Technology in Society*, 64, 101515. https://doi.org/10.1016/j.techsoc.2020.101515

2. Liu, Y. L., Yan, W., & Hu, B. (2021). Resistance to facial recognition payment in China: the influence of privacy-related factors. *Telecommunications Policy*, 45(5), 102115. https://doi.org/10.1016/j.telpol.2021.102155

3. iimedia (2019). Facial payment research report in China. https://www.iimedia.cn/c400/66866.html

4. Allen, K. (2019). China facial recognition: Law professor sues wildlife park. BBC News. https://www.bbc.com/news/world-asia-china-50324342

5. Maity, S., Abdel-Mottaleb, M., & Asfour, S. S. (2020). Multimodal biometrics recognition from facial video with missing modalities using deep learning. *Journal of Information Processing Systems*, 16(1), 6–29. https://doi.org/10.3745/JIPS.02.0129

6. Dibeklioglu, H., Alnajar, F., Salah, A. A., & Gevers, T. (2015). Combining facial dynamics with appearance for age estimation. *IEEE Transactions on Image Processing*, 24(6), 1928–1943. https://doi.org/10.1109/TIP.2015.2412377

7. Dantcheva, A., & Brémont, F. (2016). Gender estimation based on smile-dynamics. *IEEE Transactions on Information Forensics and Security*, 12(3), 719–729. https://doi.org/10.1109/TIFS.2016.2632070

8. Zhang, W. K., & Kang, M. J. (2019). Factors affecting the use of facial-recognition payment: An example of Chinese consumers. *Ieee Access : Practical Innovations, Open Solutions*, 7, 154360–154374. https://doi.org/10.10110/ACCESS.2019.2927705

9. Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: measuring individuals’ concerns about organizational practices. *MIS Quarterly*, 20(2), 167–196. https://doi.org/10.2307/249477

10. Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, 81(APR.), 42–51. https://doi.org/10.1016/j.chb.2017.12.001

11. Cheng, X., Hou, T., & Mou, J. (2021). Investigating perceived risks and benefits of information privacy disclosure in it-enabled ride-sharing. *Information & Management*, (2), 103450. https://doi.org/10.1016/j.im.2021.103450

12. Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS Quarterly*, 35(4), 989–1016. https://doi.org/10.2307/4109970

13. Li, L., Lee, K. Y., Chang, Y., Yang, S. B., & Park, P. (2021). IT-enabled sustainable development in electric scooter sharing platforms: focusing on the privacy concerns for traceable information. *Information Technology for Development*, (2), 1–24. https://doi.org/10.1080/02681102.2021.1882366

14. Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy calculus model in e-commerce – a study of Italy and the United States. *European Journal of Information Systems*, 15(4), 389–402. https://doi.org/10.1057/palgrave.ejis.3000590

15. Zhu, M., et al. (2021). Privacy paradox in mHealth applications: an integrated elaboration likelihood model incorporating privacy calculus and privacy fatigue. *Telematics and Informatics*, 61, 101601

16. Hargittai, E., & Marwick, A. (2016). “What can I really do?”: explaining the privacy paradox with online apathy. *International Journal of Communication*, 10, 3737–3757

17. Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the qualitative-quantitative divide: guidelines for conducting mixed methods research in information systems. *MIS Quarterly*, 37(1), 21–54. https://www.ijost.org/handle/43825936

18. Venkatesh, V., Brown, S. A., & Sullivan, Y. W., et al. (2016). Guidelines for conducting mixed-methods research: an extension and illustration. *Journal of the Association of Information Systems*, 17(7), 435–495. https://doi.org/10.17705/1jais.00433

19. Galton, F. (1889). Head growth in students at the University of Cambridge. *Nature*, 40, 318. https://doi.org/10.1038/040318a0

20. Galton, F. (1910). Numerical profiles for classification and recognition. *Nature*, 83, 127–130. https://doi.org/10.1038/083127a0

21. Morosan, C. (2020). Hotel facial recognition systems: insight into guests’ system perceptions, congruity with selfimage, and anticipated emotions. *Journal of Electronic Commerce Research*, 21(1), 21–38
22. Gao, J., Rong, Y., Tian, X., & Yao, Y. O. (2020). Save time or save face? the stage fright effect in the adoption of facial recognition payment technology. *Social Science Electronic Publishing*, [https://doi.org/10.2139/ssrn.3668036](https://doi.org/10.2139/ssrn.3668036)

23. Moriuchi, E. (2021). An empirical study of consumers’ intention to use biometric facial recognition as a payment method. *Psychology & Marketing*, [https://doi.org/10.1002/mar.21495](https://doi.org/10.1002/mar.21495)

24. Ciftci, O., Choi, E., & Berezina, K. (2021). Let’s face it: are customers ready for facial recognition technology at quick-service restaurants? *International Journal of Hospitality Management*, 95(2), 102941. [https://doi.org/10.1016/j.ijhm.2021.102941](https://doi.org/10.1016/j.ijhm.2021.102941)

25. Xu, Z., Zhang, T., Zeng, Y., Wan, & Wu, W. (2015, March). A secure mobile payment framework on face authentication. *The International Multiconference of Engineers and Computer Scientists*

26. Belanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS Quarterly*, 35, 1017–1041. [https://doi.org/10.2307/41409971](https://doi.org/10.2307/41409971)

27. Bansal, G., & Zahedi, F. M. (2015). Trust violation and repair: the information privacy perspective. *Decision Support Systems*, 71(1), 62–77. [https://doi.org/10.1016/j.dss.2015.01.009](https://doi.org/10.1016/j.dss.2015.01.009)

28. Milten, C. L., & Smith, H. J. (2015). Exploring information privacy regulation, risks, trust, and behavior. *Information & Management*, 52(6), 741–759. [https://doi.org/10.1016/j.im.2015.06.006](https://doi.org/10.1016/j.im.2015.06.006)

29. Ursin, G., Malila, N., Chang-Claude, J., Gunter, M., & Knudsen, G. (2019). Sharing data safely while preserving privacy. *The Lancet*, 394(10212), 1902. [https://doi.org/10.1016/S0140-6736(19)32603-0](https://doi.org/10.1016/S0140-6736(19)32603-0)

30. Agozie, D. Q., & Kay, T. (2021). Discerning the effect of privacy information transparency on privacy fatigue in e-government. *Government Information Quarterly*, 1, 101601. [https://doi.org/10.1016/j.giq.2021.101601](https://doi.org/10.1016/j.giq.2021.101601)

31. James, T. L., Wallace, L., Warkentin, M., Kim, B. C., & Collignon, S. E. (2017). Exposing others’ information on online social networks (OSNs): perceived shared risk, its determinants, and its influence on OSN privacy control use. *Information & Management*, 54(7), 851–865. [https://doi.org/10.1016/j.im.2017.01.001](https://doi.org/10.1016/j.im.2017.01.001)

32. Yu, L., Li, H., He, W., Wang, F. K., & Jiao, S. (2019). A meta-analysis to explore privacy cognition and information disclosure of internet users. *International Journal of Information Management*, 51, 102015. [https://doi.org/10.1016/j.ijinfomgt.2019.09.011](https://doi.org/10.1016/j.ijinfomgt.2019.09.011)

33. Cellary, W., & Rykowski, J. (2015). Challenges of smart industries – privacy and payment in visible versus unseen internet. *Government Information Quarterly*, 35(4), S17-S23. [https://doi.org/10.1016/j.giq.2015.08.005](https://doi.org/10.1016/j.giq.2015.08.005)

34. Krishen, A. S., Raschke, R. L., Close, A. G., & Kachroo, P. (2017). A power-responsibility equilibrium framework for fairness: understanding consumers’ implicit privacy concerns for location-based services. *Journal of Business Research*, 73(4), 20–29. [https://doi.org/10.1016/j.jbusres.2016.12.002](https://doi.org/10.1016/j.jbusres.2016.12.002)

35. Xu, H., Teo, H. H., Tan, B., & Agarwal, R. (2009). The role of push-pull technology in privacy calculus. *Journal of Management Information Systems*, 26(3), 135–174. [https://doi.org/10.2753/MIS0742-122260305](https://doi.org/10.2753/MIS0742-122260305)

36. Son, J. Y., & Kim, S. S. (2008). Internet users’ information privacy-protective responses: a taxonomy and a nomological model. *MIS Quarterly*, 32(3), 503–529

37. Ream, E., & Richardson, A. (1996). Fatigue: a concept analysis. *International Journal of Nursing Studies*, 33(5), 519–529

38. D’Urso, S. C. (2010). Who’s watching us at work? toward a structural–perceptual model of electronic monitoring and surveillance in organizations. *Communication Theory*, 16(3), 281–303. [https://doi.org/10.1111/j.1468-2885.2006.00271.x](https://doi.org/10.1111/j.1468-2885.2006.00271.x)

39. Sirka, L. J., & Dorothy, E. L. (1999). Communication and Trust in Global Virtual Teams. *Organization Science, 10*(6), 791–815. [https://www.jstor.org/stable/2640242](https://www.jstor.org/stable/2640242)

40. Anthony, D. M., & Krishnamurthy, S. (2002). Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions[J]. *The Journal of Consumer Affairs, 36*(1), 28–49. [https://www.jstor.org/stable/23860158](https://www.jstor.org/stable/23860158)

41. Moon, Y. (2000). Intimate exchanges: using computers to elicit self-disclosure from consumers. *Journal of Consumer Research, 26*(4), 323–339. [https://doi.org/10.1086/209566](https://doi.org/10.1086/209566)

42. Dinev, T., Smith, H. J., McConnell, et al. (2015). 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](https://doi.org/10.1287/isre.2015.0600)

43. Lankton, N. K., & Tripp, J. F. (2013). A Quantitative and Qualitative Study of Facebook Privacy using the Antecedent-Privacy Concern-Outcome Macro Model. *AMCIS 2013 Proceedings*
1. Wunderlich, P., Veit, D. J., & Sarker, S. (2019). Adoption of sustainable technologies: a mixed-methods study of german households. *MIS Quarterly, 42*(2), 673–691. https://doi.org/10.25300/MISQ/2019/12112

2. Strauss, A. L., & Corbin, J. M. (2008). *Basics Of Qualitative Research: Techniques and procedures for developing grounded theory* (3rd ed.). Los Angeles: Sage Publications

3. Bansal, G., Zahedi, F., ‘, & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems, 49*(2), 138–150. https://doi.org/10.1016/j.dss.2010.01.010

4. Yuan, L. (2014). The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. *Decision Support Systems, 57*, 343–354. https://doi.org/10.1016/j.dss.2013.09.018

5. Nathalie, B., Pattyn, A., et al. (2008). “Psychophysiological investigation of vigilance decrement: Boredom or cognitive fatigue?”. *Physiology & Behavior, 93*(1–2), 369–378. https://doi.org/10.1016/j.physbeh.2007.09.016

6. Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing, 19*(1), 27–41. https://doi.org/10.1509/jppm.19.1.27.16941

7. Anić, I. D., Škare, V.; Kursan Milaković, & Ivana (2019). The determinants and effects of online privacy concerns in the context of e-commerce. *Electronic Commerce Research & Applications, 36*, 100868. https://doi.org/10.1016/j.elerap.2019.100868

8. Gardner, M., & Steinberg, L. (2005). Peer influence on risk taking, risk preference, and risky decision making in adolescence and adulthood: an experimental study. *Developmental Psychology, 41*(4), 625–635. https://doi.org/10.1037/0012-1649.41.4.625

9. Rubaltelli, E., Scrimin, S., Moscardino, U., Priolo, G., & Buodo, G. (2018). Media exposure to terrorism and people’s risk perception: the role of environmental sensitivity and psychophysiological response to stress. *British Journal of Psychology, 109*(4), 656–673. https://doi.org/10.1111/bjop.12292

10. Gu, J., Xu, Y., Xu, H., Zhang, C., & Ling, H. (2016). 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

11. 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

12. Culinan, M. J. (1993). “How Did They Get My Name?”: An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use. *MIS Quarterly, 17*(3), 341–363. https://doi.org/10.2307/2497775

13. Culinan, 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.400090204

14. 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
65. Phelps, J. E., D’Souza, G., & Nowak, G. J. (2001). Antecedents and consequences of consumer privacy concerns: an empirical investigation (p2-17). *Journal of Interactive Marketing, 15*(4), 2–17. https://doi.org/10.1002/dir.1019

66. Xu, H., et al. (2012). Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services. *Information Systems Research, 23*(4), 1342–1363, 1378, 1382–1383. https://www.jstor.org/stable/42004260

67. Du, S., Keil, M., Mathiassen, L., Shen, Y., & Tiwana, A. (2007). Attention-shaping tools, expertise, and perceived control in it project risk assessment. *Decision Support Systems, 43*(1), 269–283. https://doi.org/10.1016/j.dss.2006.10.002

68. Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation. *Organization Science, 10*(1), 104–115. https://doi.org/10.1287/orsc.10.1.104

69. Chang, Y., Wong, S. F., Libaque-Saenz, C. F., & Lee, H. (2018). The role of privacy policy on consumers’ perceived privacy. *Government Information Quarterly, 445–459*. https://doi.org/10.1016/j.giq.2018.04.002

70. Liu, C., Marchewka, J. T., Lu, J., & Yu, C. S. (2005). Beyond concern—a privacy-trust-behavioral intention model of electronic commerce. *Information & Management, 42*(2), 289–304. https://doi.org/10.1016/j.im.2004.01.002

71. Huang, S. Y., Yen, D. C., & Irina Popova. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior, 28*(3), 889–897. https://doi.org/10.1016/j.chb.2011.12.008

72. Balapour, A., Nikkhah, H. R., & Sabherwal, R. (2020). Mobile application security: Role of perceived privacy as the predictor of security perceptions. *International Journal of Information Management, 52*, 102063. https://doi.org/10.1016/j.ijim.2019.102063

73. Tsai, J. Y., Egelmann, S., Cranor, L., & Acquisti, A. (2007). The effect of online privacy information on purchasing behavior: an experimental study. *Information Systems Research, 22*(2), 254–268. https://www.jstor.org/stable/23015560

74. Riahi-Belkaoui, A., & Pavlik, E. (1992). *Accounting for Corporate Reputation.* Westport, CT: Quorum Books

75. Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: the role of trust, perceived risk, and their antecedents. *Decision Support Systems, 44*(2), 544–564. https://doi.org/10.1016/j.dss.2007.07.001

76. Josang, A., Ismail, R., & Boyd, C. (2007). A survey of trust and reputation systems for online service provision. *Decision Support Systems, 43*(2), 618–644. https://doi.org/10.1016/j.dss.2005.05.019

77. Wermers, R. (1999). Mutual fund herding and the impact on stock prices. *The Journal of Finance, 54*(2), 581–622. https://doi.org/10.1111/0022-1082.00118

78. Brown, B. B., & Larson, J. (2009). *Peer Relationships in Adolescence.* In L. Steinberg & R. M. Lerner (Eds.), Handbook of Adolescent Psychology

79. Liang, H., & Shen, F. (2018). Birds of a schedule flock together: social networks, peer influence, and digital activity cycles. *Computers in Human Behavior, 82*(may), 167–176. https://doi.org/10.1016/j.chb.2018.01.016

80. Zhu, Z., Wang, J., Wang, X., & Wan, X. (2016). Exploring factors of user’s peer-influence behavior in social media on purchase intention: evidence from qq. *Computers in Human Behavior, 63*, 980–987. https://doi.org/10.1016/j.chb.2016.05.037

81. Hoadley, C. M., Xu, H., Lee, J. J., & Rosson, M. B. (2010). Privacy as information access and illusory control: the case of the Facebook news feed privacy outcry. *Electronic Commerce Research & Applications, 9*(1–6), 50–60. https://doi.org/10.1016/j.elerap.2009.05.001

82. 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), 798–824. https://doi.org/10.1080/15294702.2011.101104893

83. Stone, E. F., Gueutal, H. G., Gardner, D. G., & Mcclure, S. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of Applied Psychology, 68*(3), 459–468. https://doi.org/10.1037/0021-9010.68.3.459

84. Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research, 13*(1), 36–49. https://www.jstor.org/stable/23015822

85. Okazaki, S., Eisend, M., Plangger, K., Ruyter, K. D., & Grewal, D. (2020). Understanding the strategic consequences of customer privacy concerns: a meta-analytic review. *Journal of Retailing. https://doi.org/10.1016/j.jretai.2020.05.007*
86. Bandara, R. J., Fernando, M., & Akter, S. (2021). Construing online consumers’ information privacy decisions: the impact of psychological distance. *Information & Management, 58*(7), 103497. https://doi.org/10.1016/j.im.2021.103497

87. Choi, B., & Land, L. (2016). The effects of general privacy concerns and transactional privacy concerns on Facebook apps usage. *Information & Management, 53*(7), 868–877. https://doi.org/10.1016/j.im.2016.02.003

88. Zhang, X., Liu, S., Chen, X., Wang, L., Gao, B., & Zhu, Q. (2018). Health information privacy concerns, antecedents, and information disclosure intention in online health communities. *Information & Management, 55*(4), 482–493. https://doi.org/10.1016/j.im.2017.11.003

89. Zoonen, L. V. (2016). Privacy concerns in smart cities. *Government Information Quarterly, 33*(3), 472–480. https://doi.org/10.1016/j.giq.2016.06.004

90. Hopstaken, J. F., Linden, D., Bakker, A. B., & Kompier, M. (2015). A multifaceted investigation of the link between mental fatigue and task disengagement. *Psychophysiology, 52*(3), 305–315. https://doi.org/10.1111/psyp.12339

91. Slyke, C., Shim, J. T., Johnson, R., & Jiang, J. (2006). Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems, 7*(6), 415–444. https://doi.org/10.17705/1jais.00092

92. Ax, S., & Gregg, V. H., D Jones (2001). Coping and illness cognitions: chronic fatigue syndrome. *Clinical Psychology Review, 21*(2), 161–182. https://doi.org/10.1016/S0272-7358(99)00031-8

93. Arkes, H. R., & Blumer, C. (1985). The psychology of sunk cost. *Organizational Behavior & Human Decision Processes, 35*(1), 124–140

94. Sekaran, U., & Bougie, R. (2010). *Research methods for business: A skill building approach* (5th ed.). UK: Wiley & Sons Ltd

95. Mittelstaedt, R. A., et al. (1976). Optimal Stimulation Level and the Adoption Decision Process. *Journal of Consumer Research, 3*(2), 84–94. https://www.jstor.org/stable/2489114

96. Hair, J., Mathews, M. L., & Mathews, L. R. (2017). PLM-SEM or CB-SEM: Updated guidelines on which method to use. *International Journal of Multivariate Data Analysis, 1*(2), 107–123

97. Hair, J., Sarstedt, M., Ringle, C. M., & Mená, J. A. (2012). An assessment of the use of partial least squares structural equation modeling in marketing research. *Journal of the Academy of Marketing Science, 40*(3), 414–433. https://doi.org/10.1007/s11747-011-0261-6

98. Kline, R. B. (2005). *Principles and practice of structural equation modeling* (2nd ed.). The Guilford Press

99. Saprikis, V., & Avlogiaris, G. (2021). Modeling users’ acceptance of mobile social commerce: the case of ‘Instagram checkout’. *Electronic Commerce Research, 1–30.* https://doi.org/10.17705/s10660-021-09499-4

100. Fraenkel, J. R., & Wallen, N. E. (2000). *How to design and evaluate research in education*. New York: McGraw-Hill

101. Davidshofer, K. R., & Murphy, C. O. (2005). *Psychological testing: Principles and applications*. New Jersey: Pearson/Prentice-Upper Saddle River

102. Hair, J. F. Jr., Anderson, R. E., Tatham, R. L., & Black, W. C. (2013). *Multivariate data analysis* (7th ed.). Pearson New International: Pearson Education Limited

103. Bagozzi, R. P. (1981). Evaluating structural equation models with unobservable variables and measurement error: a comment. *Journal of Marketing Research, 18*(3), 375–381. https://doi.org/10.2307/3150979

104. Gefen, D., Straub, D. W., & Boudreau, M. (2000). Structural equation modeling and regression: guidelines for research practice. *Communication of the Association for Information Systems, 4*(7), 1–77. https://doi.org/10.17705/ICAIS.00407

105. Fornell, C., & Larcker, D. F. (1981). Structural equation models with unobservable variables and measurement error: algebra and statistics. *Journal of Marketing Research, 18*(1), 39–50. https://doi.org/10.2307/3151312

106. Falk, R. F., & Miller, N. B. (1992). *A primer for soft modeling*. Akron, OH: University of Akron Press

107. Li, Y. (2011). Empirical studies on online information privacy concerns: Literature review and an integrative framework. *Communications of the Association for Information Systems, 28*(28), 453–496

108. Benamati, J. H., Ozdemir, Z. D., & Smith, H. J. (2017). An empirical test of an Antecedents - Privacy Concerns -Outcomes model. *Journal of Information Science, 43*(5), 583–600

109. Ioannou, A., Tussyadiah, I., & Yang, L. (2020). Privacy concerns and disclosure of biometric and behavioral data for travel. *International Journal of Information Management, 54*, 102122
Publisher’s Note  Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.