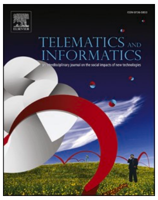
Telematics and Informatics 61 (2021) 101601

Contents lists available at ScienceDirect

Telematics and Informatics

journal homepage: www.elsevier.com/locate/tele



# Privacy paradox in mHealth applications: An integrated elaboration likelihood model incorporating privacy calculus and privacy fatigue

Mengxi Zhu [a,1], Chuanhui Wu [a,1], Shijing Huang [a], Kai Zheng [b], Sean D. Young [b], Xianglin Yan [a], Qinjian Yuan [a,*]

[a] *School of Information Management, Nanjing University, Nanjing, China*
[b] *Donald Bren School of Information and Computer Sciences, University of California, Irvine, CA, USA*

ARTICLE INFO

*Keywords:*
mHealth applications
Privacy paradox
Privacy calculus
Privacy fatigue
ELM

ABSTRACT

As people's health awareness and standard of living improve, mHealth applications are being increasingly used. However, mHealth application services are mainly based on the collection of personal and behavioral data, which conflicts with users' growing privacy concerns. In that context, this study considers the privacy paradox phenomenon, in which privacy concerns co-exist with disclosure behavior. This study explores the privacy paradox in mHealth applications using an integrated elaboration likelihood model (ELM) from the perspective of privacy calculus and privacy fatigue. Results from the quasi-experiment and partial least squares structural equation modeling reveal that, compared with privacy concerns, perceived benefits have a greater impact on users' disclosure intention, which further supports the existence of the privacy paradox in the mHealth context; this process is found to originate in users' privacy calculus. However, privacy fatigue is found to have an insignificant impact on users' disclosure intention, which may be due to the low sunk cost of users' investment in mHealth applications. The results indicate that designers of mHealth applications should optimize their interaction functions to enhance benefits to users.

## 1. Introduction

The World Health Organization (WHO) has defined mHealth as a "medical and public health service supported by mobile devices, such as smartphones, tablet computers, and other wireless devices" (Bradway et al., 2019). As effective vehicles for such services, mHealth applications are considered to be able to effectively provide safe, accessible, efficient, and low-cost health care services through continuous health monitoring, feedback, and behavior prediction (Kim et al., 2019b; Nyende, 2019). Furthermore, as people's health awareness and standard of living continue to improve, they are more interested in using mHealth applications. Data show that mHealth applications already have more than 71 million monthly active users in China, and the market value of mHealth is forecast to

* Corresponding author at: School of Information Management, Nanjing University, No. 163, Xianlin Avenue, Qixia District, Nanjing, 210023, China.

*E-mail addresses:* sissi199502@163.com (M. Zhu), dg1814017@smail.nju.edu.cn (C. Wu), 532883641@qq.com (S. Huang), zhengkai@uci.edu (K. Zheng), syoung5@hs.uci.edu (S.D. Young), yxl2441@sina.com (X. Yan), yuanqj@nju.edu.cn (Q. Yuan).

[1] Mengxi Zhu & Chuanhui Wu share the first authorship.

https://doi.org/10.1016/j.tele.2021.101601
Received 7 July 2020; Received in revised form 28 January 2021; Accepted 3 March 2021
Available online 10 March 2021

reach more than $100 billion by 2025.[2]

A major concern is that most of the medical and health services delivered by mHealth applications rely on personal data and information provided by users, which could potentially be misappropriated. Even though users' data privacy concerns are relatively low, as are the penalties for such infringements, such misappropriation does violate users' rights and benefits (Chen et al., 2018a; Li et al., 2020). Moreover, while on the one hand A privacy paradox exists as a result of users' privacy concerns and the need to disclose personal information to avail mHealth services, which could potentially endanger its further development, on the other hand they need to disclose their relevant personal information in order to use mHealth applications; this creates a privacy paradox, which could endanger the continued development of mHealth services (Adjerid et al., 2018).

This privacy paradox is very much present in the context of the health-related use of information systems (ISs) (Park and Shin, 2020). It is important to understand this paradox as privacy concerns may dictate how users interact with health-related technologies and affect ultimate health outcomes, as people with greater privacy concerns may avoid using them (Lohr, 2015). Many previous studies have explored the possible antecedents of the privacy paradox, including the herd effect (Wiedermann et al., 2014), emotions (Berendt et al., 2005), individual cognitive characteristics (Gerber et al., 2018), and the trade-off between risk and benefit (Li et al., 2019). Moreover, the existing research also covers different domains, including e-commerce (Lee et al., 2015; Kobsa et al., 2016; Karwatzki et al., 2017), social media (Taddicken, 2014; Hallam and Zanella, 2017; Chen and Cheung, 2018), and health care (Guo et al., 2015). Hitherto, the privacy paradox in the context of medical and health care has mainly focused on online health communities (Kosyfaki et al., 2017), while health service systems for mobile terminals have rarely been discussed. This literature gap prompts our current research, wherein we try to answer two research questions:

RQ1: Is there a privacy paradox in mHealth applications?

RQ2: If so, how does this phenomenon arise?

We investigate these two questions using data collected from a quasi-experimental design. First, we design an orthogonal experiment for different attributes of variables, and devise text materials and service interfaces according to the privacy environment of various mHealth applications. Then we generate eight groups of different scenario combinations and conduct a questionnaire survey.

Our study differs from prior research in three aspects. First, from a theoretical perspective, this study extends the ELM to privacy decision-making mechanism in mHealth context. In health management ISs, the user's privacy decision-making process follows central and peripheral routes. Along the central route, the user's privacy decision-making is based on in-depth, logical, and rational analyses according to their perceived advantages and disadvantages. At the same time, there is also a peripheral route, which is more dependent on heuristic evaluation for its decision-making and is influenced by such factors as mood, overall feelings, situational factors, or other behaviors. Second, we believe this study is also the first to explore the privacy paradox phenomenon from the perspective of privacy fatigue. Third, this study uses a quasi-experimental design, rather than a traditional questionnaire, to collect data, so as to better reflect real psychological states and reduce retrospective bias.

The remainder of this paper is organized as follows. In Section 2, we review related theories. In Section 3, we develop our hypotheses based on the ELM and relationships between variables. In Section 4, we describe our methods of data collection and processing. In Section 5, we analyze the empirical results. Finally, in Section 6, we summarize the main findings, implications, and limitations of this study.

## 2. Theoretical background

### 2.1. Multidimensional developmental theory

Multidimensional developmental theory (MDT) is an integrated sociological theory that explains individuals' perceptions of privacy and privacy invasion (Laufer and Wolfe, 1977). MDT theorizes that the concept of individuals' privacy concerns can be described as a consequence of self-image, environmental impact, and interpersonal interaction (Lwin and Williams, 2003). Most importantly, as the core aspect of the MDT, the interpersonal interaction dimension is focused on the relations between the individual and others, which is consistent with the dyadic exchange between individuals' use of ISs and mobile applications (Hoehle et al., 2019). There are two main components of the interpersonal interaction dimension: interaction management and information management. Interaction management refers to how an individual manages his or her interaction with others, while information management refers to how an individual manages his or her personal information. Hong and Thong (2013) identified the key dimensions and factor structure of internet privacy concerns based on MDT, including interaction management, information management, and awareness. Moreover, (Hoehle et al., 2019) showed that adhering to mobile device application usability principles could alleviate privacy concerns caused by the information and interaction management features of mobile applications, thereby improving shopping efficiency. Consistent with previous studies, we also use the interaction and information management dimensions to describe the dyadic exchange between users and mHealth applications and explore their impact on privacy-related attitudes. Specifically, in the mHealth context, information management features refer to how users understand and manage their personal information through privacy policies and privacy settings, while interaction management features refer to how users manage their interactions with the system through data transparency, interactivity, and personalization.

[2] Research report on the development trend of China's health management industry in 2017–2022. https://www.chyxx.com/research/201706/530220.html.

### 2.2. Privacy calculus

Privacy in health information could be regarded as a multidimensional form of capital that encourages protective actions (Park and Chung, 2017). As such, privacy calculus is often considered to be a rational decision-making reckoning, whereby individuals weigh up the benefits of disclosing their personal information against its costs and potential risks (Lee et al., 2013; Hoffmann et al., 2016). In online settings, the privacy calculus is further divided into privacy concerns (operationalization of costs) and benefits (Trepte et al., 2020). More importantly, most previous studies have focused on the application of privacy calculus to online disclosure intentions within different contexts, including social networks (Sun et al., 2015; Jozani et al., 2020; Trepte et al., 2020), mobile location-based advertising (Gutierrez et al., 2019), mobile applications (Morosan and DeFranco, 2015; Wang et al., 2016), and the Internet of Things (Kim et al., 2019a). Despite reported high levels of privacy concern in many contexts, consumers still readily submit their personal information (Smith et al., 2011). The privacy paradox of users' enjoying customized services while risking losing some of their personal information is evident in the mobile setting, as the success of any innovative mobile applications or service depends on the acquisition of personal information (Wang et al., 2016). Moreover, research also suggests that consumers do not pay much attention to perceived privacy risks when providing the privacy information that is a prerequisite for obtaining more personalized services (Kim et al., 2019b).

### 2.3. Privacy fatigue

Fatigue is defined as a "subjective, unpleasant feeling of tiredness that has multiple dimensions varying in duration, unpleasantness, and intensity" (Piper et al., 1987, p. 19). Fatigue is a widespread negative psychological state experienced by students, teachers, social media users, and others (Dhir et al., 2019). Specifically, in the context of online privacy, users often suffer from privacy fatigue for two reasons: first, increasingly complicated privacy assurance protocols require users to invest more cognitive effort to understand them; second, frequently disclosing highly granular personal information to many information-based service providers also makes users feel that they are losing control over their personal information (Choi et al., 2018). As a result, users may eventually feel a sense of futility and psychological stress when considering their privacy. In addition, users may employ a negative coping mechanism to protect themselves from privacy concerns. They may also put less effort into making privacy-related decisions as a result of privacy fatigue (Lutz et al., 2020). Choi, Park, and Jung (2018) have identified positive links between privacy fatigue and disengagement, suggesting that people experiencing high levels of privacy fatigue tend to do nothing to prevent the misuse of their personal information.

### 2.4. Affordance

In the field of human–computer interaction, affordance is considered to be a possibility that the environment offers for action, provided that participants know how to interact with artifacts or environments (Norman, 1999; Gibson and Pick, 2000). Zhao et al. (2020) developed the concept of affordance from the IS perspective, suggesting that affordance can be regarded as an analytical tool to study how individuals seek and use information and how systems and services affect their information behaviors. The nomological framework that links affordance with privacy mainly pertains to social media. Our perception of social media privacy may be the result of a "warm" and "cold" affordance interaction: "warm" affordance refers to the interaction function of social media, which allows us to share, keep in touch, or interact with others, whereas "cold" affordance refers to the fact that social media rely on the legal framework that sets out the terms and conditions of their use (Trepte, 2015). In other words, it is an affordance that enables social media to deal with complex privacy and security issues (Santos and Faure, 2018). Moreover, empirical evidence has also demonstrated that affordance could enhance users' social capital directly or indirectly through privacy disclosure (Proudfoot et al., 2018; Shane-Simpson et al., 2018).

### 2.5. Elaboration likelihood model

The ELM is based on the dual-process model of human cognition in cognitive psychology (Neys, 2012). Specifically, human thinking can be characterized as an interplay of an intuitive-heuristic system with a deliberate-analytic system. The former mainly relies on prior knowledge, experience, and belief, whereas the latter relates to concepts, logic, and rational thinking. Based on the dual processing theory, the ELM proposed by (Petty and Cacioppo, 1986) suggested that there are "central" and "peripheral" routes to persuasion, and that the path taken depends on the depth and efforts of the individual's cognitive processing. Specifically, the central route refers to processes that require high levels of cognitive effort, while the peripheral route refers to processes that require less cognitive effort and can be influenced by other factors (Chen et al., 2018b). ELM is widely used by IS scholars for studying situations in which persuasion could occur, such as online marketing and user adoption (Zhou, 2012; Cyr et al., 2018; Han et al., 2018).

In the electronic health-related context, previous studies mostly focused on the antecedents of user adoption to various health ISs by ELM, including electronic patient care report systems (Yoo et al., 2020), online follow-up service (Li et al., 2021), mHealth service (Meng et al., 2019), mHealth applications (Chen et al., 2018b), and electronic health records (Angst and Agarwal, 2009). Specifically, there are two main categories of factors that are highlighted in the existing research, argument quality, and source credibility. Argument quality is often regarded as the central route since it is related to objective assessment on the accuracy and completeness of the information (Meng et al., 2019; Yoo et al., 2020), while source credibility is considered as peripheral route as it is more related to the surround rather than the strength of the contents (Li et al., 2021). Moreover, it is also suggested that attitudes and concern for information privacy may affect the likelihood of users' adoption (Angst and Agarwal, 2009; Chen et al., 2018b; Gu et al., 2017; Li et al., 2021).

Although privacy decision-making in the online environment is different from privacy decision-making in the advertising or marketing environments, the method by which external information is processed is similar. In health-related ISs, we argue that users' privacy decision-making processes similarly follow both central and peripheral routes. Specifically, the central route processes the evidence related to information, which requires time and effort to investigate, while the peripheral route uses sample cues such as source factors, emotional status, or inductive reasoning to evaluate the validity of the information provided (Petty et al., 1997). We argue that in the context of mHealth, information management may require using more cognitive resources than interaction management, as users need to spend much more effort and time evaluating, understanding, and scrutinizing information (Chen et al., 2018b). Furthermore, the information management feature is more related to objective analysis and assessment on the accuracy, completeness, and relevancy of the information, as well as the validity of reasoning in the argument to form the judgment. However, the interaction management feature is related to the peripheral route, because it entails fewer cognitive resources, and it is more related to a general impression or other surface-level features than the strength of the content (Yooet al., 2020).

## 3. Research framework and hypothesis development

### 3.1. Central route: Information management features

#### 3.1.1. Information management and privacy fatigue

Along with emotional exhaustion, cynicism is a core dimension of privacy fatigue, which mainly develops from a failure to experience expected outcomes (Choi et al., 2018). Privacy cynicism is defined as an uncertain, powerless, and distrustful attitude toward the processing of personal information by online services (Lutz et al., 2020). As a cognitive coping mechanism, privacy cynicism allows users to benefit from online services without experiencing cognitive dissonance (Hoffmann et al., 2016). According to the consistency theory, when users feel threatened or stressed, they will actively change their cognition of the problem to reduce their stress, although the actual situation remains unchanged (Strachan et al., 2009). Encountering the increasingly serious problem of Internet privacy, users instinctively adopt this emotion-centered coping mechanism, which actively increases their adaptive cognitive distance from privacy issues through privacy fatigue and reduces their discomfort. Previous studies have suggested that fatigue is generated by the mismatch between system environment settings and user capabilities, as well as between user efforts and system returns (Harden, 1999; Maslach et al., 2001). In the mobile application environment, the obscure, complex system privacy policies and system privacy functions often play such a role.

**H1** Privacy policy effectiveness has a negative impact on privacy fatigue;

**H2** Privacy setting affordance has a negative impact on privacy fatigue.

#### 3.1.2. Information management and privacy calculus

The privacy system in mobile applications attempts to ensure users' information privacy. It includes two functions: the first is the system privacy policy of informing users how their personal information is collected, used, and shared with third parties; the second manages the functioning authority, data authority, information display, and interactions with applications.

An effective privacy policy will significantly reduce the degree of users' privacy concerns, improve their security experience (Wirtz et al., 2007), and by doing so, strengthen their belief in privacy rights (Anic et al., 2018). Li et al. (2016) discussed the factors influencing acceptance of wearable technology devices and pointed out that high levels of legal protection can effectively reduce users' risk concerns and enhance their willingness to accept technology. Therefore, it can be inferred that effective privacy policies in mHealth applications can also reduce users' privacy concerns, enhance their trust and perception of the benefits of using the applications.

**H3a** Privacy policy effectiveness has a positive impact on perceived benefits;

**H3b** Privacy policy effectiveness has a negative impact on privacy concerns.

In the social media context, perceived affordance has become the major factor driving perceived social benefits and disclosure intention (Proudfoot et al., 2018). Such affordance enables social media to cope with complex privacy and security issues by IS artifacts or settings (Santos and Faure, 2018). For instance, (Shane-Simpson et al., 2018) demonstrated that user-adjustable privacy settings could promote the social capital of users and increase, rather than decrease, the information they disclose. Moreover, providing users with alternative privacy disclosure options will enhance users' perceived fairness of the program settings and increase their control over personal privacy information (Wang and Wu, 2014). The privacy function of mobile application settings has similar characteristics. On the one hand, complicated and obscure privacy settings are difficult for users to find and understand, while allowing vendors to easily access user information. On the other hand, a privacy setting system with high affordance can reduce the cognitive cost to users by enhancing their privacy experience.

**H4a** Privacy setting affordance has a positive impact on perceived benefits;

**H4b** Privacy setting affordance has a positive impact on privacy concerns.

### 3.2. Peripheral route: Interaction management features

Data transparency is a general practice requirement. Transparent information collection and dissemination processes help users make informed decisions. For most users, privacy has the attributes of rights and property (Mireille and Serge, 2008). If a service's privacy settings are not transparent, the service provider or a third party will have the opportunity to make profits through the user's personal data. Although data transparency is not a completely unified concept, there are certain commonalities in each system; for example, ISs have to provide certain information on how data is processed or used. ISs with different levels of data transparency have different degrees of information security (Dayana et al., 2020). Some studies have divided the transparency characteristics of healthcare communication into three dimensions: research purpose, information form, and research time limit. Their results have shown the negative effect of these dimensions on users' privacy risk perception (Esmaeilzadeh, 2019). Moreover, while exploring the information diffusion processes of mHealth applications for diabetes patients, (Zhilian et al., 2020) has pointed out that only 4.9% of the applications meet the requirements of information transparency and that the opaque health information processes will deepen users' distrust and increase users' privacy awareness. In mHealth applications, the level of data transparency reflects the advantages and disadvantages of system privacy security. On the one hand, in an environment with poor data transparency, users are more likely to perceive unsafe factors and pay more attention to application privacy. On the other hand, users are more likely to understand a transparent application's data collection and processing settings. At the same time, it also becomes easier for users to find the data and its sources, which enhances their sense of trust, experience, and convenience.

**H5a** Data transparency has a positive impact on perceived benefits;

**H5b** Data transparency has a negative impact on privacy concerns.

Mobile Internet allows speedy information exchange and strong data connectivity; an increasing number of mobile applications choose to add user interaction functions to enhance their sense of belonging, increase user activity and generated content, and improve the users' convenience and the richness of their experience (Oestreicher-Singer and Zalmanson, 2013). Online interactive communication can support ordinary users dealing with health issues and reduce the pressure they may face when communicating health problems offline. For instance, teenagers may prefer to consult other users on online platforms about physiological changes in adolescence and women may prefer to consult other users online about menstruation and pregnancy (Wright et al., 2003; Oh, 2012). The interaction process can also offer social support, including not only effective information support from professionals, but also emotional support from other users. However, at the same time, the spread of information and unrestricted data reading also increases the user's privacy concerns. Kavianpour et al. (2019) pointed out that, while social media obtain a large amount of user interaction information, they also disseminate user data to third parties to obtain relevant services and profits, and that such uncontrolled information diffusion may further endanger user privacy. Similarly, in mHealth applications, some operators have chosen to create user interaction functions to promote the exchange and dissemination of health information, which also increases users' privacy concerns.

**H6a** System interaction has a positive impact on perceived benefits;

**H6b** System interaction has a positive impact on privacy concerns.

Personalization refers to applications' ability to filter information content in advance, based on users' data and behavior information, to adapt to their preferences (Chellappa and Sin, 2005). The widespread use of big data technology provides development opportunities for in-depth data analysis and advanced personalized services. Some mHealth applications also use personalized services to meet the diversified needs of users, such as personalized delivery of relevant healthcare information according to the health status of the user. Personalized services can collect, organize, and classify resources into various channels, turn passive searches into active recommendations, save users' time when they are searching for information, and improve their satisfaction and usage intention. However, although personalized service has many advantages, it necessarily requires users to disclose more personal information. George et al. (2002) demonstrated that, in an e-commerce environment, users will have a sense of privacy invasion if they find that the shopping lists they see are based on their personalized browsing and purchase history. Further, Guo et al. (2015) suggested that personalized services can significantly improve users' perceptions of privacy issues in mHealth services and affect how willing they are to accept technology. Notwithstanding these factors, personalized service improves the usability and satisfaction of applications and, while it may lead to misuse and abuse of privacy, the background mechanism of the service may depend on users' private data.

**H7a** System personalization has a positive impact on perceived benefits;

**H7b** System personalization has a positive impact on privacy concerns.

### 3.3. *Privacy fatigue and disclosure intention*

It is suggested that individuals with fatigue are more likely to reduce their decision-making efforts (Levav et al., 2010), such behavior can also be regarded as a manifestation of users' privacy fatigue, as they may not be willing to devote major endeavors to managing the information they share (Choi et al., 2018). In the information era, the sharing and dissemination of personal information have become particularly easy and users can exchange their personal information for high-quality services, closer relationships, and practical benefits. Therefore, it is difficult to effectively protect user privacy and complex privacy management processes impose a burden on users' cognition and energy. Privacy fatigue reflects users' weariness and powerlessness regarding privacy issues (Hargittai and Marwick, 2016). Users with privacy cynicism want to reduce their decision-making workload, so they tend to choose the simplest method of dealing with the issue by, for example, accepting default privacy settings (Schomakers et al., 2019). Choi et al. (2018) also found that privacy fatigue has a significant positive impact on privacy disclosure intention. It can be inferred that when users are tired of privacy issues, they are more likely to disclose their personal data to the system.

**H8** Privacy fatigue has a positive impact on disclosure intention.

### 3.4. *Privacy calculus and disclosure intention*

Various studies have explored the relationship between perceived benefits, privacy concerns, and disclosure intentions based on privacy calculus theory (PCT). Dienlin and Metzger, (2015) explored the antecedents of self-disclosure and self-separation of Facebook users and found that perceived benefits and privacy concerns have positive and negative impacts on users' self-disclosure intention, respectively. Cho, Ko, and Lee (2018) suggested that the higher the perceived benefits of wearable health devices, the more will users willingly disclose information and vice versa. Similar research results have been obtained in different research contexts, such as location-based services (Keith et al., 2013), e-commerce (Teubner and Flath, 2019), and online advertising (Gironda and Korgaonkar, 2018). Therefore, it can also be inferred that in mHealth applications, perceived benefits and privacy concerns have a similar impact on users' disclosure intention. According to PCT, when the benefits of privacy are greater than its costs, users tend to disclose their privacy; otherwise, they tend to keep their information private. Owing to the existence of the privacy paradox, we believe that in mHealth applications the impact of perceived benefits on disclosure intention is greater than the impact of privacy concerns on disclosure intention, which makes users disclose their privacy even if they have strong privacy concerns.

**H9** Perceived benefits have a positive impact on disclosure intention;

**H10** Privacy concerns have a negative impact on disclosure intention;

**H11** Compared with privacy concerns, the effect of perceived benefits on disclosure will be greater.

Our investigative model is illustrated in Fig. 1.

## 4. Methodology and data collection

### 4.1. *Quasi-experimental design*

This study uses a quasi-experimental design instead of a traditional questionnaire to emulate the actual environment wherein users make most of the decisions; this also helps improve the reliability of the research data. The quasi-experimental design is mainly divided into two parts: situation combination design and situation material design. The combination of eight situations describes different attributes of each variable based on an orthogonal experimental design and the situation material design displays the text material and application service interface according to the actual privacy environment of a variety of mHealth applications, which can be found in the Appendix.

Considering that our research was conducted in China, we translated all items into Chinese following a translation committee's approach (Van De Vijver, 1997). We first invited two doctoral students with different backgrounds (ISs, psychology) to complete the translation of the questionnaire items independently. We then invited a professor from the School of Foreign Language (who was not told about the purpose of this study) to translate the questionnaire items independently. Finally, the first two doctoral students compared the translated texts and no significant semantic ambiguity was found.

### 4.2. *Measurement*

The measurement of variables is based on previous research and adapted to the context of mHealth. We used a five-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly disagree). The specific items, descriptions, and sources used can be found in the Appendix.

### 4.3. *Data collection*

Before the formal data collection exercise, we carried out a small-scale pre-survey. Eighty questionnaires (10 for each scenario) were collected through online platforms, of which 68 remained after the elimination of invalid questionnaires. Based on the data obtained from the questionnaire survey and follow-up interviews with the subjects, the following items were modified: 1) the items with smaller factor loadings were deleted; 2) some explanatory descriptions were added to some picture materials of the scenario description; 3) questions designed to reveal contradictory responses were added to the questionnaire to improve the accuracy and effectiveness of the questionnaire data.

The data were collected through various social media platforms, such as WeChat, Weibo, and QQ. A total of 393 final responses were collected. To ensure the quality of the sample data, the following criteria for deleting invalid questionnaires were formulated: 1) respondents filled in the questionnaire too quickly (in less than 120s); 2) respondents supplied contradictory responses to certain questions; 3) the answers on the questionnaire were all identical. After eliminating the invalid questionnaires, 251 questionnaires were remained, which equates to a response rate of 63.9%. The demographics of the sample are displayed in Table 1.

The demographics of the sample are in line with the user profiles obtained in a market survey.[3] Most users of mHealth applications are highly educated, young people, who pay attention to self-management and scientific guidance and are willing to accept the convenience of emerging technology. Therefore, the sample population characteristics of this study are consistent with those of the existing and potential users of mHealth applications, which shows that the sample is, to a considerable degree, representative of users of mHealth applications.

[3] Research report on the development trend of China's health management industry in 2017–2022. https://www.chyxx.com/research/201706/530220.html.

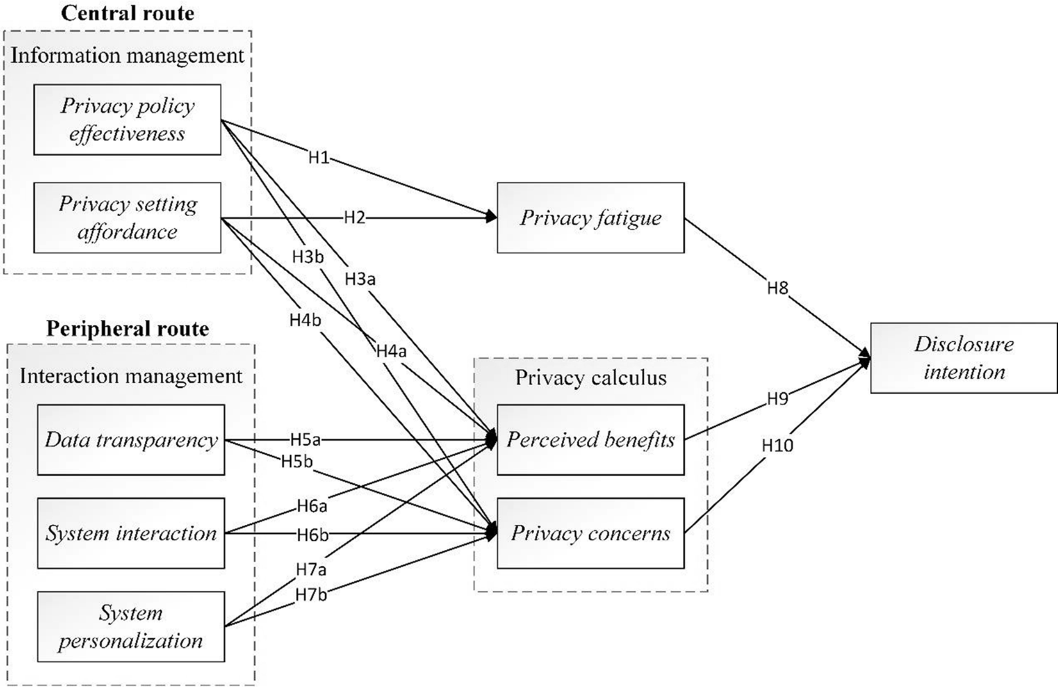


**Fig. 1.** Research model.

**Table 1**
Demographics.

| Variable | Items | Frequency | Percentage |
|---|---|---|---|
| Gender | Male | 101 | 40.20% |
| | Female | 150 | 59.80% |
| Age | Under 18 | 2 | 0.80% |
| | 18–25 | 143 | 57.00% |
| | 26–30 | 38 | 15.10% |
| | 31–40 | 38 | 15.10% |
| | 41 and above | 30 | 12.00% |
| Education | High school | 10 | 4.00% |
| | College | 24 | 9.60% |
| | bachelor | 122 | 48.60% |
| | Master | 83 | 33.10% |
| | Ph.D. and above | 12 | 4.80% |
| Experience with mHealth applications | 1–6 months | 82 | 32.70% |
| | 6–12 months | 26 | 10.40% |
| | 1–2 years | 37 | 14.70% |
| | 2–3 years | 29 | 11.60% |
| | Over 3 years | 27 | 10.80% |
| | Never | 50 | 19.90% |
| Used applications(*Top 5*) | Keep | 162 | 62.80% |
| | Xiaomi sport | 68 | 26.40% |
| | Apple health | 53 | 20.50% |
| | Huawei health | 50 | 19.40% |
| | Yuedong sport | 45 | 17.40% |

## 5. Results

### 5.1. Common method variance

We tested for common method variance since our data were collected from the same source, measurement environment, and context. Harman's single-factor method was applied to address this concern, and the results revealed that eight constructs had eigenvalues greater than 1.0, explaining 82.40% of the variance, which indicates that common method variance is not obvious and does not have a serious impact on the robustness of the results.

### 5.2. Measurement model

We used confirmatory factor analysis (CFA) to verify the reliability and validity of the constructs. The results, shown in Table 2, demonstrate that Cronbach's alpha ranged from 0.705 to 0.967 and the composite reliability ranged from 0.843 to 0.979, which are all above the benchmark value of 0.7. Moreover, the average variance extracted (AVE) values ranged from 0.628 to 0.915 and were also higher than the benchmark value of 0.5. These results show that the measurement model has good convergent validity and reliability.

We also tested the discriminant validity of the measurement model, as shown in Table 3. The square root of the AVEs for the potential variable is larger than the inter-construct correlation coefficient. Moreover, the inter-construct correlations ranged from −0.308 to 0.551, which is below the benchmark value of 0.71. These results also show that the measurement model has satisfactory discriminant validity.

### 5.3. Privacy paradox

To further explore the existence of the privacy paradox and exhibit it more intuitively in mHealth applications, we drew a scatter diagram of the relationship between privacy concern and disclosure intention by referring to (Schomakers et al., 2019). As demonstrated in Fig. 2, the horizontal and vertical coordinates show the attitudes of the subjects to privacy concerns and disclosure intentions, and the color depth of the points represents the frequency. Based on the typological research methods of Butler et al. (1971) and Schomakers et al. (2019b), the quadrants in the graph represent privacy pragmatists (top left), privacy apathy (bottom left), privacy paradoxes (top right), and privacy guardians (bottom right). From a comparison of the four quadrants, we can observe that the scatter points in the figure are concentrated in the upper right area, which implies that a considerable proportion of the respondents show a high degree of privacy concern and tend to disclose their information to mHealth applications. Hence, the existence of a privacy paradox in this context is confirmed.

### 5.4. Structural model

In this study, the partial least squares method was selected to evaluate the fitting of the sample data and the subsequent path test for the following reasons: 1) it can predict and estimate the small sample size; 2) it can predict and estimate data that do not conform to the normal distribution; and 3) it can predict and estimate a model with a more complex structure. Specifically, we carried out the subsequent inspection of the model based on the smartPLS 3.0 software, and the results show that the model has a good fit ($R^2$ ranged from 0.16 to 0.50, $Q^2$ ranged from 0.13 to 0.39). Because the sample data do not conform to the normal distribution, and some of the variables in the model have complex correlations with each other, it is impossible to use parameter estimation to verify whether the path coefficient is significant, making it necessary to use a bootstrapping method to test the path (Efron, 2000). As a result, the bootstrapping method ($N = 1000$) in smartPLS 3.0 was used for the hypothesis path test and the results are presented in Fig. 3. Moreover, given that some of our sample demographics might have affected the results of the structural model (specifically, gender, education, types, and experience), we estimated them as control variables in the investigated model. The final results suggested that none of these variables had a significant effect on the results.

Specifically, both privacy policy effectiveness ($\beta$ = -0.258, $p < .01$) and privacy setting affordance ($\beta$ = -0.244, $p < .001$) had a significantly positive link with privacy fatigue; hence, H1 and H2 were both supported. With regard to the relationship between information management and privacy calculus, the privacy policy effectiveness ($\beta = 0.190$, $p < .01$) and privacy-setting affordance ($\beta = 0.179$, $p < .01$) had a significantly positive relationship with perceived benefits. Moreover, the negative links between the two dimensions and privacy concerns were also verified. As a result, H3a, H3b, H4a, and H4b were all supported. In terms of the association between interaction management features and privacy calculus, the empirical results suggested that data transparency ($\beta = 0.243$, $p < .001$), system interaction ($\beta = 0.139$, $p < .05$), and system personalization ($\beta = 0.318$, $p < .001$) had a significantly positive relationship with perceived benefits, supporting H5a, H6a, and H7a. Such significantly positive links were not found in the relationships of these variables with privacy concerns; hence, H5b, H6b, and H7b were all rejected. Furthermore, there was no significant relationship

**Table 2**
Results of confirmatory factor analysis.

| Construct | Items | Cronbach's Alpha | CR | AVE |
|---|---|---|---|---|
| DI | 3 | 0.705 | 0.843 | 0.628 |
| PPE | 3 | 0.953 | 0.970 | 0.915 |
| DT | 3 | 0.921 | 0.950 | 0.864 |
| PB | 4 | 0.924 | 0.946 | 0.815 |
| PC | 4 | 0.953 | 0.966 | 0.876 |
| PF | 3 | 0.863 | 0.901 | 0.752 |
| PSA | 3 | 0.967 | 0.979 | 0.939 |
| SI | 3 | 0.954 | 0.970 | 0.915 |
| SP | 3 | 0.948 | 0.967 | 0.906 |

**Notes:** DI = disclosure intention, PPE = privacy policy effectiveness, DT = data transparency, PB = perceived benefits, PC = privacy concerns, PF = privacy fatigue, PSA = privacy setting affordance, SI = system interaction, SP = system personalization, CR = Composite Reliability, AVE = Average Variance Extraction.

**Table 3**
Means, standard deviations, and correlations.

| | Mean | SD | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| DI | 3.43 | 0.900 | **0.792** | | | | | | | | |
| PPE | 3.38 | 1.083 | 0.352 | **0.956** | | | | | | | |
| DT | 3.35 | 1.364 | 0.171 | 0.250 | **0.930** | | | | | | |
| PB | 3.76 | 0.797 | 0.472 | 0.414 | 0.469 | **0.903** | | | | | |
| PC | 3.57 | 0.991 | −0.241 | −0.296 | 0.047 | −0.149 | **0.936** | | | | |
| PF | 3.06 | 0.977 | −0.171 | −0.279 | 0.035 | −0.211 | 0.551 | **0.867** | | | |
| PSA | 3.34 | 1.248 | 0.313 | 0.292 | 0.080 | 0.371 | −0.308 | −0.441 | **0.969** | | |
| SI | 3.39 | 1.171 | 0.291 | 0.216 | 0.370 | 0.43 | −0.048 | 0.023 | 0.174 | **0.957** | |
| SP | 3.43 | 1.095 | 0.233 | 0.254 | 0.351 | 0.558 | −0.089 | −0.095 | 0.294 | 0.396 | **0.952** |

Note: The diagonal elements are the square roots of the AVEs.

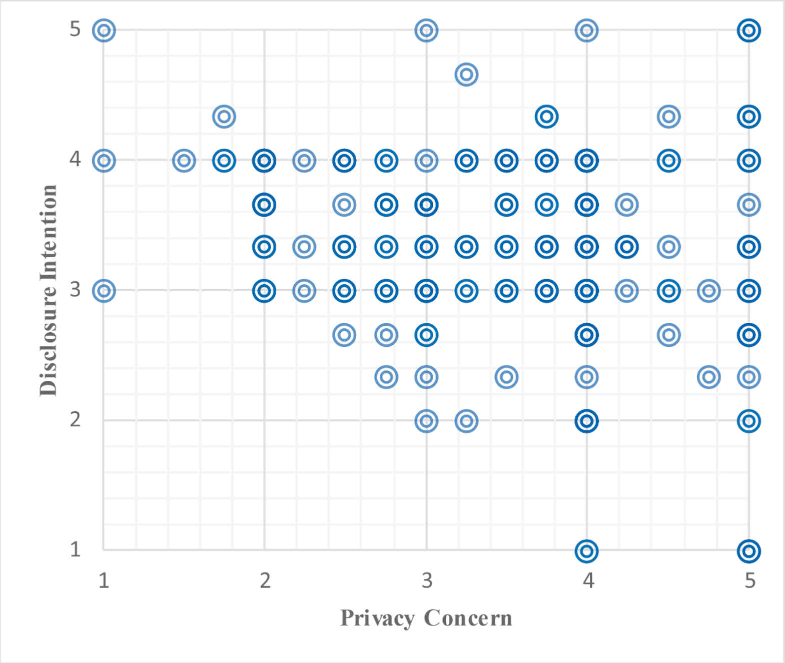


**Fig. 2.** Scatter diagram of privacy concern/disclosure intention.

between privacy fatigue and disclosure intention; hence, H8 was not supported. However, significant links between privacy calculus and disclosure were identified, supporting H9 and *H*10. Moreover, the coefficient of perceived benefits was more significant than that of privacy concerns ($|\beta 1|$ 0.449 > $|\beta 2|$ 0.196), supporting H11.

### 5.5. *Mediating effect tests*

Given that privacy concerns, perceived benefits, and privacy fatigue play an intermediary role in the relationship between interpersonal dimensions and disclosure intention, we used parallel multiple mediations to test the mediating effect, because multiple intermediary variables affect the relationship between independent and dependent variables simultaneously and there is no interaction between intermediary variables (Preacher and Hayes, 2018). Moreover, considering that the sample data do not meet the requirements of a normal distribution and the data size is relatively small, we used the bootstrapping method ($n = 1000$) for the test (Nitzl et al., 2017; Zhao and Chen, 2010). The results are shown in Table 4.

As the direct effect is added to the multiple mediating tests and a path with no significant effect affects other paths, we also brought relationships showing a marginally significant *p*-value ($p < .1$) into the discussion to obtain more enlightening results. There are four mediation paths, SI → PC → DI, SP → PC → DI, PPE → PF → DI, and PSA → PF → DI, which were not significant and not consistent with the previous results of the structural model. However, the indirect effects of DT → PB → DI, SI → PB → DI, and SP → PB → DI were significant and complete, as the direct effect between them is not significant. The direct effects of PPE → PC → DI, PSA → PC → DI, PPE → PB → DI, and PSA → PB → DI are significant and partially complementary because the direct effect and indirect effect are of the same sign.

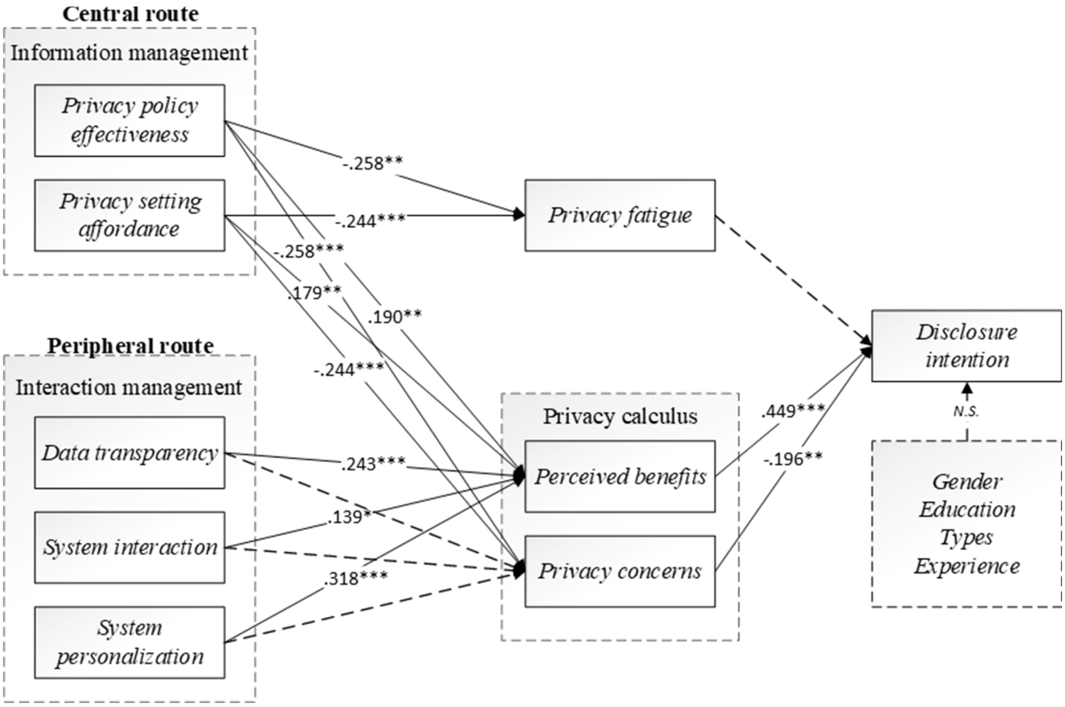


**Fig. 3.** Results of structural model (*$p < 0.05$,**$p < 0.01$,***$p < 0.001$, *N.S.*, Not significant).

**Table 4**
Results of the mediating effect.

| IV | MV | DV | Direct effect | Indirect effect | Sig. | Types of mediation |
|---|---|---|---|---|---|---|
| DT | PC | DI | −0.077 | −0.018 | N.S. | No |
| SI | | | 0.123 | 0.000 | N.S. | No |
| SP | | | −0.087 | 0.000 | N.S. | No |
| PPE | | | 0.149+ | 0.036+ | * | Partial |
| PSA | | | 0.122+ | 0.034+ | * | Partial |
| DT | PB | | −0.077 | 0.095** | ** | Full |
| SI | | | 0.123 | 0.058+ | * | Full |
| SP | | | −0.084 | 0.123** | ** | Full |
| PPE | | | 0.149+ | 0.076* | * | Partial |
| PSA | | | 0.122+ | 0.072* | * | Partial |
| PPE | PF | | 0.149+ | −0.012 | N.S. | No |
| PSA | | | 0.122+ | −0.030 | N.S. | No |

IV: independent variables; MV: mediating variables; DV: dependent variable; Sig.: significance; $^{+}p < 0.1$, *$p < 0.05$, $^{**}p < 0.01$, $^{***}p < 0.001$

## 6. Discussion

### 6.1. Key findings

This study yields various interesting findings. First and foremost, compared with privacy concerns, perceived benefits were found to have a greater impact on disclosure intention ($|\beta_1| = 0.449 > |\beta_2| = 0.196$), which further indicates the existence of the privacy paradox in mHealth applications. This process largely follows the central route through privacy calculus: specifically, the stronger the perceived interests of users, the more likely they are to disclose personal information in mHealth applications and vice versa. In addition, whether directly or indirectly, the effect of perceived benefits is stronger than that of privacy concerns, which demonstrates that users pay more attention to and weigh more heavily, the benefits of using mHealth applications rather than the costs.

Second, interaction management features have a significant positive impact on perceived benefits, which further indicates that the main demand and purpose of users using health-related ISs is to obtain their health data more transparently, directly, and quickly. However, interaction management features have no significant effect on privacy concerns. We interviewed some respondents to find an explanation for absence of such a relationship and can summarize our findings: 1) their understanding of ISs is relatively weak; 2) the interaction design of mHealth applications has been widely used in other contexts; 3) the information disclosed will not cause serious consequences; 4) respondents had no previous experience of ISs, from which it can be inferred that users' privacy concerns may arise from prior, individual experience rather than information literacy, as mHealth applications are still in the development stage.

Third, contrary to our expectations and previous results, privacy fatigue does not promote users' disclosure intention. We conducted further interviews to explain this phenomenon and they revealed that one important reason for the behavior difference between previous research scenarios and the mHealth application scenario may be caused by different sunk costs, which refers to irrecoverable costs incurred in the past, such as the time, money, and effort invested in something (Arkes and Blumer, 1985). In e-commerce, social media, and other scenarios, users have invested a lot of time, money, and cognitive effort and even have deeply embedded social links with other users, leading to a very high sunk cost. In such applications, privacy fatigue, as a coping mechanism, promotes disclosure behavior. However, mHealth applications are different. According to the data in Table 1, it can be observed that nearly 40% of mHealth application users have incurred low sunk costs. As they do not need to consider the little time and energy they have expended, these users may choose to stop using the application rather than continue to provide their personal information once they experience negative emotions.

### 6.2. Theoretical implications

Our research makes several theoretical contributions to the literature. First, it expands the research into user privacy decision-making paths in the field of information security by extending the privacy paradox to mHealth. In the existing literature, a rational or irrational behavior-oriented perspective is often used to study the causes of the privacy paradox. In this study, we integrate the two perspectives and construct a user privacy decision-making model that combines rational, irrational, and emotional perspectives.

Second, by applying the ELM in the privacy context of mHealth, we also verify its applicability and persuasiveness. In previous studies, the ELM has been applied to online marketing (Cyr et al., 2018), user adoption (Shankar et al., 2020), and other contexts, including mHealth user acceptance (Guo et al., 2020). However, our research expands the range of the ELM, and verifies the validity of the dual route of the ELM in the mHealth privacy context by combining privacy fatigue and privacy calculus.

Third, the present study discusses the concept of privacy fatigue both theoretically and empirically, whereas similar researches in the past have mostly been qualitative and focused on phenomenon discussion. In this study, privacy fatigue is regarded as the intermediary variable of the peripheral route and we verify the significant relationships between privacy policy effectiveness, privacy setting affordance, and users' privacy fatigue.

### 6.3. Managerial implications

The present study also provides some reference material and guidance for management practices. First, operators of mHealth applications should optimize their interaction function and enhance the user's perceived benefits. Specifically, for professional mHealth applications, clear data interface architecture and reasonable data visualization reports should be put in place. For mHealth applications, operators should consider setting up an appropriate reward mechanism, adding system feedback and targets, to encourage users to seek personalized services.

Second, given that a highly effective privacy policy can significantly improve the perceived benefits of users, operators and designers should consider improving privacy policies and aim for improved readability, simplicity, and humanization of their applications, based on openness and transparency. Furthermore, for regulators, clear laws and regulations should be established to protect personal health information. For example, the EU has introduced general data protection regulations. If enterprises are guilty of data violations, regulators can impose a fine of 20 million euros or 4% of their global revenue.

Third, as a privacy function design with high affordance can significantly improve the perceived benefits of users, operators and designers should consider providing a wider range of service function setting permissions, more comprehensively covering the privacy control needs of users; they could also provide personalized privacy settings based on users' daily use of the application.

Privacy fatigue is a double-edged sword for mHealth vendors. On the one hand, users with privacy fatigue are more likely to disclose their health information; on the other hand, privacy fatigue also indicates that the vendors' privacy mechanisms are not perfect. Although empirical evidence suggests that there is no significant relationship between privacy fatigue and disclosure intention, mHealth vendors should seriously consider the negative coping mechanism of users as the mHealth market expands. It is suggested that users with low levels of information literacy and computer self-efficacy tend to have cynicism in developing privacy fatigue (Hoffman et al., 2016). Therefore, improving privacy information literacy education is a direction worth exploring in the future.

### 6.4. Limitations and further directions

This study has some limitations. First, most of the participants in this study were between 20 and 30 years old with undergraduate or postgraduate degrees, which is consistent with the user characteristics of current mHealth applications. However, with the gradual improvement of public health awareness and the rising popularity of wearable health devices, the use of mHealth applications is bound to spread to a wider and more typical user population. Therefore, we could further expand the range of the sample population to obtain more robust results in future research.

Second, this paper focuses on the impact of internal functional characteristics of multiple mHealth applications on users' disclosure intentions. However, with the gradual development of the mHealth industry, we could also consider the impact of various other external factors and individual factors on users' privacy decision-making paths in the future.

Moreover, the research samples and contexts in the present research are mainly Chinese. As a result, the findings may be influenced by cultural features to a certain extent. For example, in Hofstadt's cultural-dimension theory, there are differences between uncertainty avoidance in various countries, which may have an impact on privacy concerns (Hofstede and Michael, 1984). Future studies could consider different cultural contexts, which can further deepen our understanding of the issues.

## Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## Appendix A. Situation design description

### A-1. Situation combination design

| | DT | SI | SP | PPE | PSA |
|---|---|---|---|---|---|
| 1 | H | H | L | L | H |
| 2 | L | H | H | L | H |
| 3 | L | L | L | H | H |
| 4 | H | H | L | H | L |
| 5 | L | L | L | L | L |
| 6 | L | H | H | H | L |
| 7 | H | L | H | H | H |
| 8 | H | L | H | L | L |

Note: H: high; L: low. DI = disclosure intention, SI = system interaction, SP = system personalization, PPE = privacy policy effectiveness, PSA = privacy setting affordance.

### A-2. Situation material description

| Variable | Level | Description |
|---|---|---|
| DI | H | Text description: you want to view the body data collected in A health. It is found that there is a special monitoring data page on the home page to show your real-time body data, accompanied by relevant instructions, as shown in the following figure.Picture description: the picture shows the monitoring data in A health file, including steps, weight, blood pressure, sleep and body temperature. The data source is marked on the right side of each data card. The blood pressure card sub page shows the detailed blood pressure value, and the purpose and related instructions of collecting blood pressure value are attached at the bottom of the page. |
| | L | Text description: if you want to view the body data collected in A health, it is found that there is no unified monitoring data display page set in the application. You spent 5 min to view among the scattered function pages, and each page did not make any clear information other than the data value. |
| DI | H | Text description: you have some health problems that you want to ask for help. During the use, the page of A health is displayed as shown in the following figure.Picture description: the picture shows a healthy system interaction functions such as information release, topic, likes, comments and private letters. When you see that someone has published topics related to body fat rate, you can choose private mail to ask relevant questions and get a reply. |
| | L | You have some health problems that you want to ask for help, but in the process of using it, it is found that A health has not opened the relevant functions like community or instant messaging. |
| SP | H | Text description: in the process of using A health, you find that the app provides home page information recommendation, training plan recommendation, health tips, etc. The system can generate your preferences based on your health record data and the history of browsing click information, and automatically match the relevant content that you may be interested in or useful to you, as shown in the following figure.Picture description: some information recommendation, training recommendation and diet recommendation functions of A health are shown in the figure. There are “personalized customization” and “recommendation” in the label of the page. |
| | L | In the process of using A health, you find that health content and services (including information, training content, health tips, etc.) are consistent for all users. |
| PPE | H | A health will provide a very complete and detailed data privacy policy guide in a prominent place when it is used for the first time. When A health uses your relevant data for the first time, it will jump out of relevant policies and give corresponding protection tips. In the privacy policy compliance assessment published by the government every year, A health ranks first. If any user questions or questions the data privacy policy of a health, a health will have full-time service personnel to give detailed answers. |
| | L | When a health is used for the first time, it will display “click login to agree to all the privacy agreements of A health” in small words next to the login button. Some media have pointed out that there is an obvious’ overlord clause ’in A health privacy agreement. Many users have questions about A health privacy policy, and have not heard any public response. |
| PSA | H | Text description: if you want to change privacy settings in A health, you will find that the privacy entrance design is in a prominent position on the personal settings page, with clear level and description. The page after the entrance click is shown in the following figure.Picture description: the healthy system permission setting and privacy setting of A health are shown in the figure. In the permission setting, the user can control the system permission functions such as application use and viewing location, camera, album, etc.; in the privacy permission setting, the user can control whether the application allows to find me through the address book, microblog, and whether the nearby people have medium privacy permission function. |
| | L | You want to change the privacy settings in A health, but it took 5 min to find the access to the privacy settings in the app, so you have to give up. |

## Appendix B. Measurement items

| Construct/source | Items |
|---|---|
| Data transparency (Karwatzki et al., 2017) | 1. I can quickly learn about the data collected by A health<br>2. I can quickly learn about the sources of data collected by A health<br>3. I can quickly understand the purposes of collecting data for A health |
| System interaction (Johnson et al., 2006) | 1. I can interact with other users' health information through A health<br>2. I can strengthen my contact with other users through A health<br>3. A health can let other users know my health |
| System personalization (Mothersbaugh et al., 2012) | 1. In general, I think A health can flexibly serve me according to my wishes<br>2. A health can adjust the service and content according to my specific needs<br>3. I can create a training plan and health information suitable for my own needs and preferences with A health. |
| Privacy policy effectiveness (Li et al., 2016) | 1. I think it's effective to show the privacy policy of A health<br>2. I think privacy policy of A health is compliant<br>3. I think the protection promised in A health is effective |
| Privacy setting affordance (Grange, 2013; Grgecic et al., 2015) | 1. I can easily find the privacy switch I need to set in A health<br>2. The process of viewing the privacy management system and using it in A health consumes less energy and time for me<br>3. The privacy system function of A health let me know how to control my privacy information<br>4. Every privacy function and information annotation of A health are well understood |
| Privacy concern (Smith and Burke, 1996; Xu et al., 2012) | 1. Using A health, I'm afraid my privacy will be violated<br>2. Using A health, I'm worried that my personal information will be over collected<br>3. Using A health, I'm worried that my personal information will be accessed without authorization<br>4. Using A health, I'm worried that my daily operations will be tracked and monitored |
| Perceived benefits (Xu et al., 2011) | 1. A healths services and functions help me save time searching for useful health information<br>2. A healths services and functions provide me with instant and convenient health information<br>3. A healths services and functions can effectively help me achieve my fitness goals<br>4. In general, the services and functions of A health are beneficial to me |
| Privacy fatigue (Choi et al., 2018) | 1. Dealing with privacy in A health is exhausting<br>2. I'm not in a good mood when I'm dealing with the privacy issues in A health<br>3. I'm not so interested in the privacy issues of the A health<br>4. I have doubts about the significance of privacy in the A health |
| Disclosure intention (Li et al., 2016; Bansal et al., 2010) | 1. In order to use the services of A health, I would like to disclose relevant data<br>2. In order to use the service of A health, I will probably disclose relevant information<br>3. In order to use the services of A health, I tend to provide relevant data |

## References

Adjerid, I., Peer, E., Acquisti, A., 2018. Beyond the privacy paradox: Objective versus relative risk in privacy decision making. MIS Quarterly 42 (2), 465–488.

Angst, C.M., Agarwal, R., 2009. Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. MIS Quarterly 33 (2), 339–370.

Anic, I.-D., Budak, J., Rajh, E., Recher, V., Skare, V., Skrinjaric, B., 2018. Extended model of online privacy concern: What drives consumers' decisions? Online Inf. Rev. 43 (5), 799–817.

Arkes, H.R., Blumer, C., 1985. The psychology of sunk cost. Organ. Behav. Hum. Decis. Process. 35 (1), 124–140.

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).

Berendt, B., Gunther, O., Spiekermnn, S., 2005. Privacy in E-commerce: Stated preferences vs. actual behavior. Commun. ACM 48 (4), 103.

Bradway, M., Carrion, C., Vallespin, B., Saadatfard, O., Puigdomènech, E., Espallargues, M., Kotzeva, A., 2019. Mhealth Assessment: Conceptualization of a global framework. JMIR Mhealth Uhealth 5 (5), e60. https://doi.org/10.2196/mhealth.7291.

Butler, M., Westin, A.F., Schiller, H.I., et al., 1971. Privacy and freedom. Int. Affairs 47 (2), 468–469.

Chellappa, R.K., Sin, R.G., 2005. Personalization versus privacy: An empirical examination of the online consumer's dilemma. Inf. Technol. Manage. 6 (2-3), 181–202.

Chen, Z.T., Cheung, M., 2018. Privacy perception and protection on Chinese social media: A case study of WeChat. Ethics Inf. Technol. 20 (4), 279–289.

Chen, Y.i., Ding, S., Zheng, H., Zhang, Y., Yang, S., 2018a. Exploring diffusion strategies for mHealth promotion using evolutionary game model. Appl. Math. Comput. 336, 148–161.

Chen, Y., Yang, L., Zhang, M., Yang, J., 2018b. Central or peripheral? Cognition elaboration cues' effect on users' continuance intention of mobile health applications in the developing markets. Int. J. Med. Inf. 116, 33–45.

Cho, J.Y., Ko, D., Lee, B.G., 2018. Strategic approach to privacy calculus of wearable device user regarding information disclosure and continuance intention. KSII Trans. Internet Inf. Syst. 12 (7), 3356–3374.

Choi, H., Park, J., Jung, Y., 2018. The role of privacy fatigue in online privacy behavior. Comput. Hum. Behav. 81, 42–51.

Cyr, D., Head, M., Lim, E., Stibe, A., 2018. Using the elaboration likelihood model to examine online persuasion through website design. Inf. Manage. 55 (7), 807–821.

Dayana, S., Bartolini, C., Gabriele, L., 2020. Qualifying and measuring transparency: A medical data system case study. Comput. Security 91, 1–20.

Dhir, A., Kaur, P., Chen, S., Pallesen, S., 2019. Antecedents and consequences of social media fatigue. Int. J. Inf. Manage. 48, 193–202.

Dienlin, T., Metzger, M.J., 2015. An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative U.S. sample. J. Comput. Mediated Commun. 21 (5), 363–383.

Esmaeilzadeh, P., 2019. Consumers' perceptions of using health information exchanges (HIEs) for research purposes. Inf. Syst. Manage. 36 (1), 57–77.

George, R., Juha, T., Koukara, L., et al., 2002. A case study in pervasive retail. Assoc. Comput. Mach. 28 (2), 90–94.

Gerber, N., Gerber, P., Volkamer, M., 2018. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. Comput. Security 77, 226–261.

Gibson, J.J., Pick, A.D., 2000. An Ecological Approach to Perceptual Learning and Development. Oxford University Press, New York.

Gironda, J.T., Korgaonkar, P.K., 2018. iSpy? Tailored versus invasive ads and consumers' perceptions of personalized advertising. Electron. Commer. Res. Appl. 29, 64–77.

Grange, Benbasat, 2013. Foundations for Investigating the drivers of the value captured by consumers embedded within social shopping networks. Proceedings of the 46th Hawaii International Conference on System Sciences.

Grgecic, D, Holten, R, Rosenkranz, C, 2015. The impact of functional affordances and symbolic expressions on the formation of beliefs. Journal of the Association for Information Systems 16 (7).

Gu, J., Xu, Y.(., Xu, H., Zhang, C., Ling, H., 2017. Privacy concerns for mobile app download: An elaboration likelihood model perspective. Decis. Support Syst. 94, 19–28.

Guo, X., Zhang, X., Sun, Y., 2015. The privacy-personalization paradox in mHealth services acceptance of different age groups. Electron. Commer. Res. Appl. 16, 55–65.

Guo, X., Chen, S., Zhang, X., Ju, X., Wang, X., 2020. Exploring patients' intentions for continuous usage of mHealth Services: Elaboration-likelihood perspective study. JMIR Mhealth Uhealth 8 (4), e17258. https://doi.org/10.2196/17258.

Gutierrez, A., O'Leary, S., Rana, N.P., Dwivedi, Y.K., Calle, T., 2019. Using privacy calculus theory to explore entrepreneurial directions in mobile location-based advertising: Identifying intrusiveness as the critical risk factor. Comput. Hum. Behav. 95, 295–306.

Hallam, C., Zanella, G., 2017. Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. Comput. Hum. Behav. 68, 217–227.

Han, J.-T., Chen, Q., Liu, J.-G., Luo, X.-L., Fan, W., 2018. The persuasion of borrowers' voluntary information in peer to peer lending: An empirical study based on elaboration likelihood model. Comput. Hum. Behav. 78, 200–214.

Harden, R.M, 1999. Stress, pressure and burnout in teachers: is the swan exhausted? Medical Teacher 21 (3).

Hargittai, E., Marwick, A., 2016. What can I really do?": Explaining the privacy paradox with online apathy. "Int. J. Commun. 10, 3737–3757.

Hoehle, H, Aloysius, J. A, Goodarzi, S, Venkatesh, V, 2019. A nomological network of customers' privacy perceptions: linking artifact design to shopping efficiency. European Journal of Information Systems 28 (1), 91–113.

Hoffmann, C.P., Lutz, C., Ranzini, G., 2016. Privacy cynicism: A new approach to the privacy paradox. Cyberpsychol. J. Psychosocial Res. Cyberspace 10 (4).

Hofstede, G., Michael, B., 1984. Hofstede's culture dimensions: An independent validation using Rokeach's value survey. J. Cross Cult. Psychol. 15 (4), 417–433.

Hong, W., Thong, J.Y.L., 2013. Internet privacy concerns: an integrated conceptualization and four empirical studies. MIS Quarterly 37 (1), 275–298.

Johnson, G.J, Bruner, G.C, Kumar, A, 2006. Interactivity and Its Facets Revisited: Theory and Empirical Test. Journal of Advertising 35 (4), 35–52.

Jozani, M., Ayaburi, E., Ko, M., Choo, K.-K., 2020. Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective. Comput. Hum. Behav. 107, 106260. https://doi.org/10.1016/j.chb.2020.106260.

Karwatzki, S., Dytynko, O., Trenz, M., Veit, D., 2017. Beyond the personalization–privacy paradox: Privacy valuation, transparency features, and service personalization. J. Manage. Inf. Syst. 34 (2), 369–400.

Kavianpour, S., Tamimi, A., Shanmugam, B., 2019. A privacy-preserving model to control social interaction behaviors in social network sites. J. Inf. Security Appl. 49, 1–8.

Keith, M.J., Thompson, S.C., Hale, J., Lowry, P.B., Greer, C., 2013. Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. Int. J. Hum Comput Stud. 71 (12), 1163–1173.

Kim, D., Park, K., Park, Y., Ahn, J.-H., 2019a. Willingness to provide personal information: Perspective of privacy calculus in IoT services. Comput. Hum. Behav. 92, 273–281.

Kim, K.-H., Kim, K.-J., Lee, D.-H., Kim, M.-G., 2019b. Identification of critical quality dimensions for continuance intention in mHealth services: Case study of onecare service. Int. J. Inf. Manage. 46, 187–197.

Kobsa, A., Cho, H., Knijnenburg, B.P., 2016. The effect of personalization provider characteristics on privacy attitudes and behaviors: An elaboration likelihood model approach. J. Am. Soc. Inform. Sci. Technol. 67 (11), 2587–2606.

Kosyfaki, C., Angelova, N.P., Tsohou, A., et al., 2017. The privacy paradox in the context of online health data disclosure by users. Inf. Syst. EMCIS 299, 426–428.

Laufer, R.S., Wolfe, M., 1977. Privacy as a concept and a social issue: A multidimensional developmental theory. J. Soc. Issues 33 (3), 22–42.

Lee, H., Lim, D., Kim, H., Zo, H., Ciganek, A.P., 2015. Compensation paradox: The influence of monetary rewards on user behaviour. Behav. Inf. Technol. 34 (1), 45–56.

Lee, H., Park, H., Kim, J., 2013. Why do people share their context information on Social Network Services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk. Int. J. Hum Comput Stud. 71 (9), 862–877.

Levav, J., Heitmann, M., Herrmann, A., et al., 2010. Order in product customization decisions: Evidence from field experiments. J. Polit. Econ. 118 (2), 274–299.

Li, C.-R., Zhang, E., Han, J.-T., 2021. Adoption of online follow-up service by patients: An empirical study based on the elaboration likelihood model. Comput. Hum. Behav. 114, 106581. https://doi.org/10.1016/j.chb.2020.106581.

Li, P, Cho, H, Goh, Z.H., 2019. Unpacking the process of privacy management and self-disclosure from the perspectives of regulatory focus and privacy calculus. Telematics and Informatics 41, 114–125.

Li, H.e., Wu, J., Gao, Y., Shi, Y., 2016. Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective. Int. J. Med. Inf. 88, 8–17.

Li, J., Zhang, C., Li, X., Zhang, C., 2020. Patients' emotional bonding with MHealth apps: An attachment perspective on patients' use of MHealth applications. Int. J. Inf. Manage. 51, 102054. https://doi.org/10.1016/j.ijinfomgt.2019.102054.

Lohr, S. 2015. The healing power of your own medical records. New York Times, B1. Retrieved from http://www.nytimes.com/2015/04/01/technology/ the-healing-power-of-your-own-medical-data.html?_r=0.

Lutz, C., Hoffmann, C.P., Ranzini, G., 2020. Data capitalism and the user: An exploration of privacy cynicism in Germany. New Media Soc. 22 (7), 1168–1187.

Lwin, M.O., Williams, J.D., 2003. A model integrating the multidimensional developmental theory of privacy and theory of planned behavior to examine fabrication of information online. Market. Lett. 14 (4), 257–272.

Maslach, C, Schaufeli, W.B, Leiter, M.P, 2001. Job burnout. Annual Review of Psychology 52 (1).

Meng, F., Guo, X., Peng, Z., Zhang, X., Vogel, D., 2019. The routine use of mobile health services in the presence of health consciousness. Electron. Commer. Res. Appl. 35, 100847. https://doi.org/10.1016/j.elerap.2019.100847.

Mireille, H., Serge, G., 2008. Profiling the European Citizen: Cross-Disciplinary Perspectives. Springer, London.

Morosan, C., DeFranco, A., 2015. Disclosing personal information via hotel apps: A privacy calculus perspective. Int. J. Hospitality Manage. 47, 120–130.

Mothersbaugh, D.L, Foxx, W.K, Beatty, S.E, et al., 2012. Disclosure antecedents in an online service context: The role of sensitivity of information. Journal of Service Research 15 (1).

Neys, D.W., 2012. Bias and conflict: A case for logical intuitions. Perspect. Psychol. Sci. 7 (1), 28–38.

Nitzl, C., Roldán, J.L., Cepeda, G., 2017. Mediation Analyses in Partial Least Squares Structural Equation Modeling, Helping Researchers Discuss More Sophisticated Models: An Abstract. Springer, Cham.

Norman, Donald A., 1999. Affordance, conventions, and design. Interaction 6 (3), 38–43.

Nyende, H. 2019. Value Co-creation in Design of mHealth Applications for Maternal Healthcare Service Delivery. In Information and Communication Technologies for Development. Strengthening Southern-Driven Cooperation as a Catalyst for ICT4D, 89-103.

Oestreicher-Singer, Gal, Zalmanson, Lior, 2013. Content or community? A digital business strategy for content providers in the social age. MIS Quarterly 37 (2), 591–616.

Oh, S., 2012. The characteristics and motivations of health answerers for sharing information, knowledge, and experiences in online environments. J. Am. Soc. Inform. Sci. Technol. 63 (3), 543–557.

Park, Yong Jin, Chung, Jae Eun, 2017. Health privacy as sociotechnical capital. Comput. Hum. Behav. 76, 227–236.

Park, Yong Jin, Shin, Donghee Don, 2020. Contextualizing privacy on health-related use of information technology. Comput. Hum. Behav. 105, 106204. https://doi.org/10.1016/j.chb.2019.106204.

Petty, R.E., Cacioppo, J.T., 1986. The elaboration likelihood model of persuasion. Adv. Exp. Soc. Psychol. 19 (1), 124–205.

Petty, Richard E., Heesacker, Martin, Hughes, Jan N., 1997. The elaboration likelihood model: Implications for the practice of school psychology. J. Sch. Psychol. 35 (2), 107–136.

Piper, B.F., Lindsey, A.M., Dodd, M.J., 1987. Fatigue mechanisms in cancer patients: Developing nursing theory. Oncol. Nurs. Forum 14 (6), 17e23.

Preacher, K.J., Hayes, A.F., 2018. Asymptotic and resampling strategiesfor assessing and comparing indirect effects in multiple mediator models. Behav. Res. Methods 40 (3), 871–891.

Proudfoot, Jeffrey G., Wilson, David, Valacich, Joseph S., Byrd, Michael D., 2018. Saving face on Facebook: privacy concerns, social benefits, and impression management. Behav. Inf. Technol. 37 (1), 16–37.

Santos, M., Faure, A., 2018. Affordance is power: Contradictions between communicational and technical dimensions of whatsapp's end-to-end encryption. Social Media + Society 4 (3).

Schomakers, Eva-Maria, Lidynia, Chantal, Ziefle, Martina, 2019. A typology of online privacy personalities. J. Grid Comput. 17 (4), 727–747.

Shane-Simpson, Christina, Manago, Adriana, Gaggi, Naomi, Gillespie-Lynch, Kristen, 2018. Why do college students prefer Facebook, Twitter, or Instagram? Site affordances, tensions between privacy and self-expression, and implications for social capital. Comput. Hum. Behav. 86, 276–288.

Shankar, Amit, Jebarajakirthy, Charles, Ashaduzzaman, Md, 2020. How do electronic word of mouth practices contribute to mobile banking adoption? J. Retailing Consumer Services 52, 101920. https://doi.org/10.1016/j.jretconser.2019.101920.

Smith, H.J, Burke, M.S, 1996. Information privacy: Measuring individuals' concerns about organizational practices. MIS Quarterly 20 (2).

Smith, H.J., Dinev, T., Xu, H., 2011. Information privacy research: An interdisciplinary review. MIS Quarterly 35 (4), 989–1015.

Strachan, S.M., Brawley, L.R., Spink, K.S., Jung, M.E., 2009. Strength of exercise identity and identity-exercise consistency: affective and social cognitive relationships. J. Health Psychol. 14 (8), 1196–1206.

Sun, Yongqiang, Wang, Nan, Shen, Xiao-Liang, Zhang, Jacky Xi, 2015. Location information disclosure in location-based social network services: Privacy calculus, benefit structure, and gender differences. Comput. Hum. Behav. 52, 278–292.

Taddicken, Monika, 2014. The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. J. Comput. Mediated Commun. 19 (2), 248–273.

Teubner, Timm, Flath, Christoph M., 2019. Privacy in the sharing economy. J. Assoc. Inf. Syst. 213–242. https://doi.org/10.17705/1jais10.17705/1jais.00534.

Trepte, S., 2015. Social media, privacy, and self-disclosure: The turbulence caused by social media's affordances. Social Media + Society 1 (1).

Trepte, Sabine, Scharkow, Michael, Dienlin, Tobias, 2020. The privacy calculus contextualized: The influence of affordances. Comput. Hum. Behav. 104, 106115. https://doi.org/10.1016/j.chb.2019.08.022.

Van De Vijver, F.J., 1997. Methods and Data Analysis for Cross-cultural Research. Sage, Thousand Oaks, CA.

Wang, Shu-Ching, Wu, Jen-Her, 2014. Proactive privacy practices in transition: Toward ubiquitous services. Inf. Manage. 51 (1), 93–103.

Wang, Tien, Duong, Trong Danh, Chen, Charlie C., 2016. Intention to disclose personal information via mobile applications: A privacy calculus perspective. Int. J. Inf. Manage. 36 (4), 531–542.

Wiedermann, Wolfgang, Niggli, Jürg, Frick, Ulrich, 2014. The Lemming-effect: Harm perception of psychotropic substances among music festival visitors. Health Risk Soc. 16 (4), 323–338.

Wirtz, Jochen, Lwin, May O., Williams, Jerome D., 2007. Causes and consequences of consumer online privacy concern. Int. J. Service Ind. Manage. 18 (4), 326–348.

Wright, Kevin B., Bell, Sally B., Wright, Kevin B., Bell, Sally B., 2003. Health-related support groups on the internet: Linking empirical findings to social support and computer-mediated communication theory. J. Health Psychol. 8 (1), 39–54.

Xu, H, Gupta, S, Rosson, M.B, 2012. Measuring mobile users' concerns for information privacy. Thirty Third International Conference on Information Systems.

Xu, H, Luo, X, Carroll, J.M, et al., 2011. The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. Decision Support Systems 51 (1).

Yoo, Chul Woo, Huang, C. Derrick, Goo, Jahyun, 2020. Task support of electronic patient care report (ePCR) systems in emergency medical services: An elaboration likelihood model lens. Inf. Manage. 57 (6), 103336. https://doi.org/10.1016/j.im.2020.103336.

Zhao, Xinshu, Lynch, John G., Chen, Qimei, 2010. Reconsidering Baron and Kenny: Myths and truths about mediation analysis. J. Consumer Res. 37 (2), 197–206.

Zhao, Y.C., Zhang, Y., Tang, J., Song, S. 2020. Affordances for information practices: theorizing engagement among people, technology, and sociocultural environments. J. Docum., ahead-of-print(ahead-of-print).

Zhilian, H., Elain, L., Josip, C., et al., 2020. Medication management Apps for diabetes: Systematic assessment of the transparency and reliability of health information dissemination. JMIR mHealth Uhealth 8 (2), 1–10.

Zhou, T., 2012. Understanding users' initial trust in mobile banking: An elaboration likelihood perspective. Comput. Hum. Behav. 28 (4), 1518–1525.