


Research on user's highly sensitive privacy disclosure intention in home intelligent health service system: A perspective from trust enhancement mechanism

DIGITAL HEALTH
Volume 9: 1–19
© The Author(s) 2023
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/20552076231219444
journals.sagepub.com/home/dhj



Shugang Li¹, Ruoxuan Li¹ , Boyi Zhu¹, Beiyan Zhang¹, Jiayi Li², Fang Liu¹ and Yanfang Wei¹

Abstract

Objective: The aim is to investigate the determinants and mechanisms that influence user's highly sensitive privacy disclosure intention (HSPDI) in home intelligent health service system (HIHSS).

Methods: This study improves the privacy calculus theory by considering the influence of service providers' trust enhancement mechanism besides benefit and risk factors and investigates their impact on users' HSPDIs. This study takes perceived valence and perceived security as the trade-off result among perceived benefits, perceived risks, financial trust enhancement mechanism, and the technical trust enhancement mechanism and suggests that perceived valence and perceived security further affect users' HSPDI in HIHSS. Moreover, the common and differential effects of the perceived justice of privacy violation compensation (PJOPVC) and the perceived effectiveness of privacy protection technologies (PEOPPTs) are studied. The structural equation model is used to analyze 204 valid samples to test the proposed model.

Results: The results show that perceived benefits and perceived risks are important predictors of perceived valence and perceived security, and further affect users' HSPDI. We find PJOPVC has a greater impact on perceived valence while PEOPPT has a greater impact on perceived security.

Conclusions: We recommend that the HSPDI of users with low perceived valence can be improved by providing privacy violation compensation while the HSPDI of users with low perceived security can be enhanced by popularizing relevant knowledge of privacy protection technologies.

Keywords

Home intelligent health service systems, privacy disclosure intention, privacy calculus theory, financial trust enhancement mechanism, technical trust enhancement mechanism

Submission date: 23 March 2023; Acceptance date: 21 November 2023

Introduction

With the deepening of population aging, the number of the elderly, the lonely elderly and the disabled elderly in China is increasing rapidly,¹ and the demand for home intelligent health service is also increasing. To improve the sense of access, well-being and security of the elderly, it has become a valuable attempt to promote home intelligent service systems based on new technologies in the

¹School of Management, Shanghai University, Shanghai, China

²Shanghai Songjiang No.2 High School, Shanghai, China

Corresponding authors:

Fang Liu, School of Management, Shanghai University, No.99 Shangda Road, Baoshan District, 200444 Shanghai, China.
Email: fiona_liu1996@163.com

Yanfang Wei, School of Management, Shanghai University, No.99 Shangda Road, Baoshan District, 200444 Shanghai, China.
Email: weiyangfang@shu.edu.cn



community context, such as fall detection systems based on the Internet of Things² and smart technologies as well as remote service monitoring systems based on block chain.³ However, an important issue facing the home intelligent health service industry is the highly sensitive privacy disclosure of users, for example, private information relating to the user's body and information about the user's behavior in sensitive situations (e.g., bathroom and bedroom). On the one hand, service providers need to capture this highly sensitive privacy to provide useful and personalized home intelligent health services to users. On the other hand, users' privacy concerns may reduce their willingness to disclose such highly sensitive privacy, which in turn may affect the adoption and promotion of smart health services at home. According to a 2021 survey, 52% of respondents expressed concern that intelligent products in healthcare could lead to threats to security and privacy.⁴ In today's modern healthcare system, the management and security of healthcare data have gained paramount importance.⁵ With the rapid advancement of healthcare information technology, the tasks of storing, transmitting, and analyzing medical data have become more streamlined and user-friendly. However, this progress also introduces potential vulnerabilities, particularly when it comes to the issues of healthcare data breaches and infringements on privacy.^{6,7} Recent research has been dedicated to harnessing computational techniques to assess the repercussions of healthcare data breaches. Almalawi et al.⁸ proposed an innovative encryption approach named "Lionized Remora Optimization-Based Serpent" to fortify the protection of sensitive data. This approach not only alleviates privacy violations and cyber threats from unauthorized users and hackers but also optimizes the efficiency of data encryption and decryption, thereby elevating the standards of privacy safeguards. Based on these technological backgrounds, analyzing privacy sharing intentions from the perspective of user privacy sharing decision-making mechanisms has also attracted the attention of scholars. In this regard, in addition to the direct risks and benefits of privacy disclosure, it is found that privacy control enhancement mechanisms such as privacy protection policies and privacy setting functions provided by service providers can improve users' privacy disclosure intention.⁹ Moreover, in order to improve users' privacy disclosure intention, service providers often provide trust enhancement mechanisms to enhance users' trust, such as privacy violation compensation and efficient privacy protection technologies, but there is still a lack of discussion in this field. Therefore, in order to improve users' willingness to disclose highly sensitive privacy under the trust enhancement mechanism of service providers and to promote the application of intelligent health services in home scenarios, this study investigates the factors and mechanisms influencing users' intention to disclose highly sensitive privacy in home intelligent health service systems (HIHSS).

Privacy calculus refers to the cognitive process of evaluating the trade-off between the benefits of sharing personal information and the potential risks of privacy infringement when individuals make decisions to disclose or conceal privacy in various situations. Privacy calculus theory is widely used in the study of privacy disclosure behavior in the field of health services,^{10,11} and it is the main theory to explain the privacy disclosure behavior of users in the internet platforms. According to the privacy calculus theory, the privacy disclosure behavior depends on the user's trade-off between the benefits of privacy disclosure and the risks of privacy disclosure.^{12,13} The first goal of this study is to study the user's highly sensitive privacy disclosure intention (HSPDI) in the HIHSS from the perspective of privacy calculus. Unlike other systems, home intelligent health services systems require users to disclose more sensitive and private information. Such private information is often related to personal freedom, dignity, and reputation. If the privacy information is disclosed, it may cause long-lasting and irreversible damage to the users' personality.¹⁴ This study helps to clarify the impact of privacy disclosure benefits privacy disclosure risks on users' intention to disclose highly sensitive privacy in the home intelligent health service scenarios, and furthermore, to provide scientific recommendations and guidance for enhancing users' intention to disclose highly sensitive privacy in the context of home intelligent healthcare service systems. In addition, understanding the risk and benefit factors that influence users' intention to disclose their privacy can help home intelligent health service providers to allocate resources appropriately to increase users' intention to make highly sensitive privacy disclosures and facilitate the adoption of intelligent health service systems in the home environment.

The second objective of this study is to investigate the common and differential effects of financial trust enhancement mechanism and technical trust enhancement mechanism on users' intention to make highly sensitive privacy disclosure. Privacy calculus theory only explains users' privacy disclosure behavior from the perspectives of expected benefits and potential risks brought by privacy disclosure behavior, ignoring the influence of other important factors.^{15,16} Literature suggests that users are more willing to disclose personal privacy when they have higher trust in service providers.^{17,18} In services that require users to disclose privacy, service providers usually adopt two trust enhancement mechanisms to strengthen users' trust: financial trust enhancement mechanism and technical trust enhancement mechanism. The financial trust enhancement mechanism refers to that the service provider provides users with interest protection through privacy violation compensation commitment while the technical trust enhancement mechanism means that the service provider provides privacy security guarantee for users through privacy protection technologies.¹⁹ Although

previous privacy-related studies have recognized the importance of financial and technical trust enhancement mechanisms,^{20,21} how these two mechanisms specifically affect users' privacy disclosure intention has not received much attention.

To remedy the shortcomings of the existing studies, this study proposes a research model to explain the HSPDI of users in a HIHSS. And, first of all, based on privacy calculus theory, this study will transfer privacy disclosure benefits and privacy disclosure risks operation into perceived benefits and perceived risks, perceived valence and perceived security respectively as a user in the cognitive and emotional balance of perceived benefits and the perceived risks, and suggest that perceived valence and perceived security further affect users' willingness to disclose highly sensitive privacy in HIHSSs. Then, considering the influence of trust enhancement mechanism, this study incorporates financial trust enhancement mechanism (privacy violation compensation) and technical trust enhancement mechanism (privacy protection technologies) into the research model, explores the common and differential effects of the perceived justice of privacy violation compensation (PJOPVC) and the perceived effectiveness of privacy protection technologies (PEOPPTs) on users' willingness to disclose highly sensitive privacy.

This study tested the above research model using structural equation model. The results show that perceived benefits and perceived risks are important predictors of perceived valence and perceived security, and perceived valence and perceived security further influence users' intention to disclose highly sensitive privacy. PJOPVC and PEOPPTs have common effect and difference effect on promoting users highly sensitive privacy disclosure, PJOPVC and PEOPPTs promote users' disclosure HSPDI by establishing good perceived valence and security, but PJOPVC has a greater impact on perceived valence, PEOPPTs has a greater impact on perceived security. This study expands privacy calculus theory and provides guidance for home intelligent health service providers to collect and use users' highly sensitive privacy information, and promotes the application of smart health services in home scenarios.

The rest of this study is organized as follows. The literature review about privacy calculus theory is presented in the literature review section. The research models and hypotheses are described in the research model section. The research method is showed in the method section. The statistical analysis is presented in the statistics analysis section. The results of the experiments are provided in the results section. The discussion of this study is shown in the discussion section. Finally, the conclusion of the study is elaborated in the last section.

Literature review

Privacy calculus theory is a common theory used to explain users' privacy disclosure behavior, and privacy leakage risk and privacy disclosure benefit are the two core concepts of this theory.^{12,13} Privacy leakage risk refers to the extent to which users believe that privacy disclosure will cause them loss, which is a belief that hinders privacy disclosure behavior.¹³ Privacy disclosure benefits refer to the benefits that users believe that privacy disclosure behavior will bring to them, which is a belief that encourages privacy disclosure behavior,¹³ and the specific form it takes depends on the context in which the disclosure occurs. The privacy calculus theory posits that individuals make disclosure decisions based on a balance of perceived risks and benefits of disclosing sensitive information, along with factors such as trust and perceived control, information needs, and contextual influences. The framework of privacy calculus theory aids in comprehending the decision-making process of users when disclosing sensitive information, as well as their concerns and deliberations concerning personal privacy rights. The behavior of privacy disclosure is positively affected by the expected privacy disclosure benefits and negatively affected by the potential privacy disclosure risks.

Research in the context of privacy calculus has mainly focused on considering the impact of risk, benefit, social and ease of use on privacy disclosure. For example, Sun et al.²² conducted a study on user privacy disclosure behavior in social e-commerce, and found that hot topic interactivity and group buying experience had a significant negative impact on privacy concern and a significant positive impact on perceived benefits, and privacy concern had a negative impact on information disclosure behavior while perceived benefits had a positive impact on information disclosure behavior. In the privacy calculus theory of social network, social benefits are given increasing amount of attention, such as establishing social relationships, obtaining social emotional support and self-expression.^{23–26} In the privacy calculus theory of mobile applications, the usefulness and ease of use of applications are emphasized.²⁷

In addition, there exists some researches considering the influence of users' trust perception and service providers' ability to protect and manage personal information on users' privacy disclosure behavior and privacy disclosure-related behavior. For example, Bol et al.¹⁷ and Leon et al.¹⁸ considered users' trust in service providers and used it as a factor other than risk and benefit factors to influence users' privacy disclosure behavior and privacy disclosure-related behavior. Nguyen et al.²⁸ investigated the relationship among perceived psychological benefits, online trust, and personal information disclosure behavior when users shop online in Vietnam, and found that perceived psychological benefits had the greatest impact on customers' online trust while both perceived

psychological benefits and online trust affected customers' personal information disclosure behavior. Dienlin et al.²⁹ considered the user's perception of personal privacy protection ability, and included privacy self-efficacy (individual's belief in their own privacy protection ability) into the privacy calculation model to explain the self-disclosure behavior and self-withdrawal behavior of Facebook users. In addition to considering privacy concerns and perceived benefits, Kim et al.²⁶ also considered the influence of users' trust in social networking service providers and their belief in the ability of service providers to manage personal information on users' behavior of disclosing personal information on social networking sites.

The sustainable development of online health communities requires users to constantly disclose their health-related privacy, so online health communities are also one of the key scenarios for the study of user privacy disclosure behavior. Zhang et al.³⁰ explored the antecedents and consequences of health information privacy concerns in online health communities and found that privacy concerns were negatively affected by two coping assessments (i.e., response efficacy and self-efficacy) and positively affected by two threat assessments (i.e., perceived vulnerability and perceived severity). Perceived health status mitigates the effects of privacy concerns and information support on individuals' willingness to disclose health information to varying degrees. Li et al.,³¹ based on the privacy calculus theory, constructed the online health community users' privacy disclosure behavior. The results showed that users' privacy disclosure behavior mainly depended on the perceived benefits such as information quality and service quality, and the perceived risks had a negative impact, but to a lesser extent. Taking the privacy calculus theory as the framework, combined with the social exchange theory and the trust theory, Wang¹⁰ constructed the influencing factor model of health information privacy disclosure intention of users in the virtual health community.

The impact of privacy concerns and information sensitivity on users' willingness to disclose personal health information has become a focus of research in the field of healthcare and wellness.³² According to existing research, privacy concerns and information sensitivity have been found to affect users' willingness to disclose information. Relevant studies have revealed individuals' high concern for privacy protection,³³ and sensitive information, such as medical history, disease diagnosis, and genetic data, particularly triggers users' privacy concerns. Therefore, individuals typically weigh the risks and benefits when considering disclosing such sensitive information.¹⁶ Personal and health information of users is generally considered highly sensitive, involving privacy rights and personal security. Research indicates that higher information sensitivity is associated with more cautious information sharing decisions, as individuals are more cautious when

disclosing personal health information. Information sensitivity is also closely related to trust and satisfaction, as users are more willing to trust healthcare service providers who can ensure information security.³⁴ Based on existing studies, privacy concerns and information sensitivity can influence users' willingness to disclose information. Generally, individuals with higher levels of privacy concerns and information sensitivity tend to be more cautious in their decision-making and inclined to protect their personal information.³⁵ In HHSs, a large amount of highly sensitive user privacy information needs to be collected. This study focuses on how to improve users' intention to disclose privacy in this scenario.

Although privacy calculus theory is a common theory to explain privacy disclosure behavior, it only explains user privacy disclosure behavior from the perspective of expected benefits and potential risks, ignoring the influence of other important factors such as service providers' trust enhancement mechanisms (i.e., mechanisms that enhance user trust) in addition to risk and benefit factors. In order to fill the research gap, based on the privacy calculus theory, this study considers the influence of service providers' trust enhancement mechanism besides benefit and risk factors.

Many scholars believe that trust has multiple dimensions, and study the dimensions of trust. Lui et al.³⁶ divided trust into two dimensions: ability and goodwill. In their study, competence included characteristics such as good reputation and capital, and goodwill included characteristics such as fairness and credit in negotiations. Mayer et al.³⁷ divided trust into three dimensions: integrity, competence, and goodwill. Among them, integrity referred to the honesty and trustworthiness of the trusted party, competence indicated the ability of the trusted party to meet the needs of the client, and goodwill represented the trust party's concern for the interests of the trusting party. McAllister³⁸ divided trust into cognitive trust and affective trust. Cognitive trust was defined as an individual's belief in the reliability, integrity and honesty of the trusted party. Affective trust reflected the responsibility, care, and concern for the welfare of the trusted party. Although there are differences in the current division of trust dimensions, many researchers believe that trust should include at least two dimensions.^{39–41} One dimension describes the benevolent or "willing to do" aspect of the trustworthiness of the trusted party, also known as goodwill-based trust.⁴² Another dimension describes the ability or "can-do" aspect of the trustworthiness of the trusted party, also known as competency-based trust.⁴³

In services that require users to disclose their privacy, the goodwill of service providers is mainly reflected by providing financial compensation for users after privacy violations while the ability of service providers is mainly reflected by providing privacy protection technologies for users. Financial trust enhancement mechanism and technical

trust enhancement mechanism are two main mechanisms for service providers to enhance user trust in services that require users to disclose their privacy.^{44,45} This study considers the impact of trust enhancement mechanism on users' disclosure intention of highly sensitive privacy in HIHSS and incorporates financial trust enhancement mechanism (privacy violation compensation) and technical trust enhancement mechanism (privacy protection technologies) into the research model. Furthermore, this study studies the common and differential effects of PJOPVC and PEOPTs on users' disclosure intention of highly sensitive privacy in HIHSS.

Research model

The research model of this study is shown in Figure 1. The impact of privacy calculus and trust enhancement mechanisms on user privacy disclosure intention in HIHSS is studied. Firstly, this study uses perceived risks and perceived benefits to represent the risks of privacy disclosure and the benefits of privacy disclosure, respectively, takes perceived valence and perceived security as the trade-off results between perceived risks and perceived benefits, and explores the impact of privacy calculus on users' willingness for privacy disclosure. Secondly, this study uses PJOPVC and PEOPTs to represent the financial trust enhancement mechanism and the technical trust enhancement mechanism, respectively, and explores the common and differential effect of the financial trust enhancement mechanism and the technical trust enhancement mechanism on users' privacy disclosure intention.

Privacy calculus

The study considers perceived valence and perceived security as privacy disclosure risk and privacy disclosure benefit trade-off results. In the context of HIHSS privacy disclosure, the potential mechanism that mediates the relationship between the independent and dependent variables is the privacy calculus theory. Traditional privacy calculus theory emphasizes that individuals weigh the benefits of information sharing against privacy risks when deciding whether to disclose privacy information. However, our research innovatively proposes using perceived valence and perceived security as mediating variables to balance the risks and benefits of privacy disclosure. Perceived valence emphasizes users' subjective perception and evaluation of data privacy protection, rather than just evaluating the benefits of using the service. By considering users' perceived valence of privacy protection as a personalized decision basis, we aim to better meet users' privacy protection needs. In privacy calculus, the innovation of perceived security, relative to the traditional risk-benefit trade-off, lies in its emphasis on users' subjective perception and evaluation of privacy protection, as well as the consideration of individual sense of security. Perceived security highlights the importance of user participation and control. In privacy calculus, users can participate in the data processing and decision-making process through authorization, permission management, and other means. These control measures can increase users' sense of security and trust.

Perceived valence refers to how people think things are beneficial or unfavorable to them, reflecting the overall

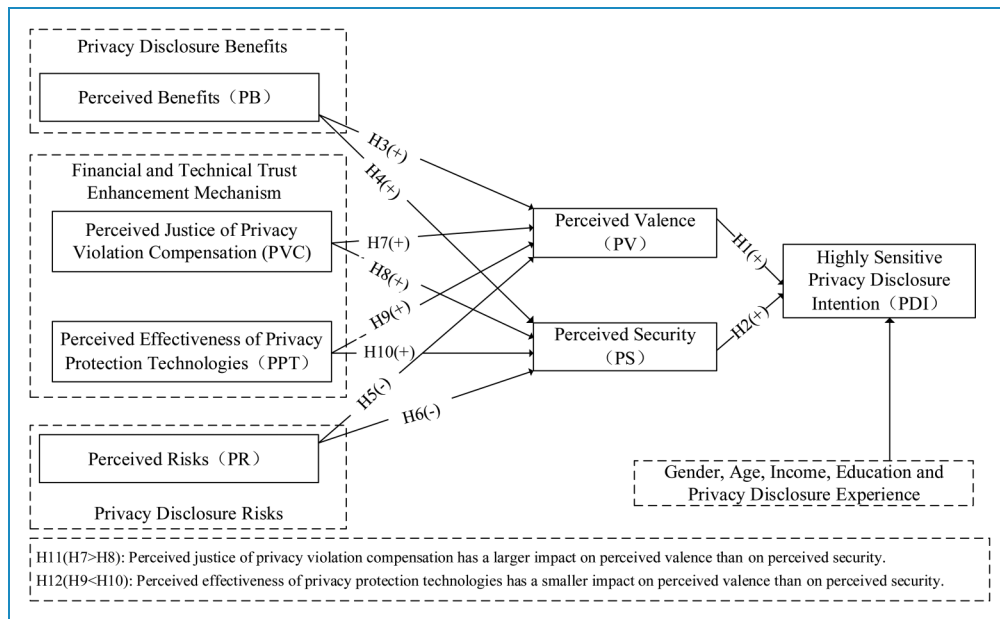


Figure 1. Influence mechanism model of user's highly sensitive privacy disclosure intention in home intelligent health service system.

attractiveness of things to the user.⁴⁶ In this study, perceived valence refers to the degree to which users believe that disclosing personal highly sensitive private information to the HIHSS is beneficial or detrimental to themselves as a whole. Home intelligent health services include fall detection,^{47–49} assisting elderly or patient bathing⁵⁰ and changing clothes.^{51,52} In order to provide these services effectively, users need to allow smart devices to collect private information related to the user's body and sensitive behavioral information in specific scenarios (such as toilets). Although sharing these highly sensitive privacy information poses potential risks, users can get personalized, intelligent health services. This kind of privacy leakage risk and privacy disclosure benefit trade-off helps users to form an overall favorable or unfavorable perception of the disclosure of highly sensitive privacy information. Users are more likely to disclose highly sensitive private information to the HIHSS when the disclosure of highly sensitive information can bring them a high level of perceived valence. Therefore, the hypothesis is:

H1: Perceived valence positively affects highly sensitive privacy disclosure intention

Akalin et al.⁵³ described perceived security as the user's perception of the level of danger while interacting with the robot, and the user's comfort level during the interaction while investigating key concepts in human–computer interaction problems. In this study, based on this description, perceived security is defined as the user's perception of danger and comfort in disclosing highly sensitive private information to the HIHSS. Home intelligent health services have the characteristics of personalized and intelligent, and can effectively meet the different needs of users. This consistency of service and demand will make users have a sense of security. Perceived security is an emotional response, a high level of perceived security means that consumers view the provision of highly sensitive private information to an HIHSS as emotionally safe and comfortable, thereby increasing the likelihood of disclosing highly sensitive private information. The existing study has also shown that users' affective responses affect the level of effort associated with cognitive processing, which in turn influences user behavior.⁵⁴ Therefore, we infer that:

H2: Perceived security positively affects highly sensitive privacy disclosure intention

In this study, perceived benefits of users disclosing highly sensitive privacy to the HIHSS are used to represent the benefits of privacy disclosure, that is, the health service provided by the HIHSS based on users' highly sensitive privacy information. In HIHSSs, when users make decisions to disclose highly sensitive information, they consider

potential benefits such as personal health monitoring, customized services, and improved medical decision support. Home based smart health services rely on the ability to collect data from a variety of sources, including the environment and the patient themselves. By using various sensors to collect highly sensitive privacy information of users, service providers can provide users with more accurate and intelligent services to meet the health service needs of specific users, such as indoor fall detection needs,⁵⁵ auxiliary dressing demands,⁵⁶ and auxiliary bathing requirements.⁵⁰ Users with a high level of perceived benefits have a higher demand for the services they can obtain, and are more inclined to make a positive judgment on the overall value of disclosing highly sensitive privacy information to the HIHSS. Therefore, it is assumed that:

H3: Perceived benefits positively affect perceived valence

In this study, perceived benefits may affect perceived security. On the one hand, as a favorable belief, perceived benefits may offset users' privacy concerns,^{57,58} thus increasing users' perception of privacy security in disclosing highly sensitive private information to the HIHSS. On the other hand, the high level of perceived benefits shows that the HIHSS can meet the needs of users, provide intelligent and personalized health services for users. In the case that this demand can be met, the user's satisfaction with the HIHSS may increase, and then produce a good psychological state. Therefore, it is assumed that:

H4: Perceived benefits positively affect perceived security

In this study, perceived risks of users disclosing highly sensitive privacy information to the HIHSS are used to represent the risks of privacy disclosure, that is, the user's estimation of the possible loss of privacy caused by disclosing highly sensitive privacy information to the HIHSS.⁵⁹ In HIHSS, users consider potential risks when deciding to disclose highly sensitive information, including privacy breaches, data misuse, information security threats, identity theft, and unauthorized access. Users are less likely to realize the value of privacy disclosure to others when they are exposed to the risk of privacy disclosure in information exchange.^{59,60} In our research scenario, highly sensitive private information, such as user behavior information in sensitive environment and image information related to the user's body, will often damage the user's dignity and cause serious psychological harm to the user if exposed to others.⁶¹ A high level of perceived risks means that users believe that disclosing their highly sensitive privacy information will cause a serious loss of privacy, which leads to a low level of overall value assessment of highly sensitive privacy disclosure. Therefore, we infer that:

H5: Perceived risks negatively affect perceived valence

Perceived risks may also affect the perceived security of users disclosing highly sensitive privacy information to the HIHSS. A high level of perceived risks implies that users lack confidence in the service provider's ability and willingness to protect their highly sensitive private information.⁶² Compared to users with a low level of perceived risks, users with a high level of perceived risks are more worried about the disclosure of highly sensitive privacy information and unauthorized use and access,⁶¹ and have a lower assessment of their overall privacy status.⁶³ These concerns about privacy information may lead to users' psychological state of anxiety and discomfort, and reduce users' perceived security. Therefore, we presume that:

H6: Perceived risks negatively affect perceived security*The common effect and differential effect of trust enhancement mechanism*

In addition to the direct risks and benefits of privacy disclosure, the trust enhancement mechanisms provided by service providers to enhance users' trust, such as privacy violation compensation and efficient privacy protection technologies, may also affect users' willingness to disclose privacy. Extant studies mainly focus on the impact of privacy control enhancement mechanisms, such as privacy protection policies and privacy setting functions, which enhance users' sense of control, on users' privacy disclosure behavior while there are few studies on trust enhancement mechanisms provided by service providers. This study investigates the common effects and differential effects of financial trust enhancement mechanism and technical trust enhancement mechanism on users' HSPDI in HIHSS.

The common effect emphasizes that the financial trust enhancement mechanism and the technical trust enhancement mechanism promote users to share highly sensitive privacy by establishing good perceived valence and perceived security. In this study, PJOPVC is used to represent the financial trust enhancement mechanism, that is, the user's perception of the justice of the financial compensation provided by the home intelligent health service provider for the user's loss after the privacy violation event. Fair compensation for privacy violations can restore the balance of personal information exchange⁶⁴ and shape users' cognitive responses to privacy issues in the online environment. For example, in a study on location-based services, Xu et al.⁶⁵ found that impartial compensation addressed negative user perceptions of location information collected by online companies. Essentially, fair privacy violation compensation can make up for the loss caused by privacy invasion events, ensure the fairness of services, and reduce users' sense of noncompliance,²¹ leading to positive judgments about the overall value of disclosing

highly sensitive privacy information to HIHSS. Therefore, it is inferred that:

H7: Perceived justice of privacy violation compensation positively affects perceived valence

Privacy violation events can cause high anxiety among users of HIHSSs about the service providers' commitment to protecting their privacy. Through financial compensation commitment, users can confirm that service providers are willing to take responsibility for privacy violation events, thus reducing users' dissatisfaction with service failure.⁶⁶ In addition, there is evidence that financial compensation can directly affect the emotional response of customers to online privacy issues. For example, Hann et al.⁶⁷ found that financial compensation reduced users' feelings of insecurity and vulnerability due to privacy violation. Choi et al.²¹ found that financial compensation was effective in alleviating users' feelings of privacy violation. Users of HIHSSs who have a high level of perceived justice in financial compensation will have a lower sense of insecurity and discomfort caused by privacy violations. Therefore, we hypothesize that:

H8: Perceived justice of privacy violation compensation positively affects perceived security

In this study, PEOPPTs is used to represent the technical trust enhancement mechanism. Referring to the research of Wang et al.,²⁰ the PEOPPTs is defined as the degree to which users of HIHSS believe that their highly sensitive privacy information can be protected by the privacy protection technologies provided by the service provider. In healthcare context, privacy protection technologies such as differential privacy and homomorphic encryption have been widely used to protect user privacy, and technologies such as block chain (e.g., anonymity, encryption technology, permission control, privacy contracts, decentralized identity verification, etc.) and federated learning are gradually applied to privacy protection.⁶⁸ Privacy protection technologies can effectively prevent unauthorized information access and collection,⁶⁹ and reduce users' privacy concerns. In order to improve the ability to develop effective and ethical approaches to building and maintaining trust in HIHSS, standardization of the above technologies has also been developed, which can involve the implementation of standardized encryption and authentication protocols to secure data transmission and storage in HIHSS devices. It can also involve the use of standardized privacy policies and consent management frameworks to ensure individuals have control over the use and sharing of their health data. The more effective the privacy protection technologies are, the smaller the possibility of privacy invasion events is, and the higher the possibility of users making favorable

value judgments on highly sensitive privacy disclosure behavior is. Therefore, we speculate that:

H9: Perceived effectiveness of privacy protection technologies positively affects the perceived valence

The PEOPTs may also affect the perceived security of users disclosing highly sensitive private information. On the one hand, privacy protection technologies can directly provide privacy protection for users of HIHSS, reduce the possibility of privacy disclosure, and enhance users' sense of security. On the other hand, emerging privacy protection technologies such as block chain can manage data sharing and data storage by providing authentication, access control, and authorization, thus improving the confidentiality and integrity of data and enhancing users' sense of control over highly sensitive personal privacy information.⁷⁰ This sense of control can effectively reduce the user's concern for privacy⁷¹ and improve the user's perceived security. Therefore, it is supposed that:

H10: Perceived effectiveness of privacy protection technologies positively affects perceived security

The difference effect shows that the financial trust enhancement mechanism (PJOPVC) and the technical trust enhancement mechanism (PEOPTs) enhance users' willingness to disclose highly sensitive privacy information to different levels through different coping processes. According to trust-related studies,^{37,72} privacy violation compensation is highly related to users' good-will-centered responses, while privacy protection technologies is highly related to users' ability-centered responses. When facing possible privacy issues, users may first conduct an ability-centered response by evaluating the privacy protection capabilities of service providers. When an ability-centered response fails to address all possible privacy issues, users may engage in a well-intention-centered response by assessing the willingness of service providers to take responsibility for privacy violation events. Ability-centered coping style helps users to produce good emotions to deal with risk situations, so it is more important for the formation of perceived security than the formation of perceived valence. Good-will-centered coping style can effectively reduce the user's expectation of the loss caused by privacy violation events, so it has a greater impact on the formation of perceived valence than perceived security. Therefore, we hypothesize that:

H11: Perceived justice of privacy violation compensation has a greater impact on perceived valence than on perceived security

H12: Perceived effectiveness of privacy protection technologies has less impact on perceived valence than on perceived security

Control variable

In addition to the above factors, other factors may also affect the highly sensitive privacy disclosure willingness of users of HIHSSs. Relevant studies have found that age, gender, income, education, and privacy violation experience play key roles in the formation of users' willingness to disclose privacy.^{73,74} In order to control these unknown effects, five control variables are added to the model, including age, gender, income, education, and privacy violation experience.

Method

Questionnaire design

This study is an empirical research on users' intention to disclose highly sensitive privacy in the context of HIHSSs. Data were collected through online survey questionnaires between July 2022 and August 2022. And the proposed model was examined using structural equation modeling (SEM). Therefore, in this study, a questionnaire containing a description of the scenario was designed,⁷⁵ which consisted of three parts. The first part investigated the basic information of the respondents, including gender, age, income, education, and privacy violation experience.

The second part was the scenario description. Scenario description method has been widely used in previous studies, which can simulate a more realistic environment and improve the realism of user decision making.⁷⁵ This study refers to the research of Kim et al.⁷⁶ and King et al.,⁵⁰ using text description and picture display to introduce a virtual usage scenario, functional characteristics, privacy protection technologies, and privacy violation compensation standard of a HIHSS, namely bed bath robot system, to help respondents establish the concept of HIHSS. Therefore, textual expressions in the description of the scenario were used to make the respondents imagine themselves as patients who are inconvenient to take a bath, such as Alzheimer's patients.

The third part was the measurement of variables related to the scenario, including seven variables: perceived benefits, perceived risks, perceived effectiveness of privacy protection technologies, perceived justice of privacy violation compensation, perceived valence, perceived security and disclosure intention of highly sensitive privacy. In this study, all variables were measured using a 7-point Likert scale ranging from "1 = strongly disagree" to "7 = strongly agree." In order to ensure the reliability and validity of the scale, the scale used for each variable is the mature scale in the relevant research. At the same time, some of the items have been modified to adapt to the background of home intelligent health service. In order to ensure the validity of the content, a group of experts was invited (including a

Table 1. Variable measurement.

Construct	Coding	Measurement Item	References
Perceived benefits (PB)	PB1	Using the system can make me safer.	35
	PB2	Using the system can improve my ability to live independently.	
	PB3	Using the system can improve my quality of life.	
Perceived effectiveness of privacy protection technologies (PPT)	PPT1	I believe the privacy protection technologies of the system are effective.	20
	PPT2	I believe the system's privacy protection technologies are reliable.	
	PPT3	I believe the system's privacy protection technologies are safe.	
Perceived justice of privacy violation compensation (PVC)	PVC1	I think the compensation offered by the service provider for the violation of privacy is fair.	21
	PVC2	I think the service provider's compensation for privacy violations is fair.	
	PVC3	I think the service provider has provided adequate compensation for privacy violations.	
Perceived risks (PR)	PR1	There is a risk of privacy disclosure when using this system.	59
	PR2	The use of this system may bring great loss of privacy.	
	PR3	Using the system may cause my privacy to be compromised.	
	PR4	The use of this system may cause many unexpected privacy problems.	
Perceived valence (PV)	PV1	I think the system will bring me a good service experience.	46
	PV2	I believe the service provider tries to give me a good service experience.	
	PV3	I believe that service providers know what kind of service experience users want.	
Perceived security (PS)	PS1	I think it's safe to disclose highly sensitive privacy in exchange for health services.	77
	PS2	I think it's safe to disclose highly sensitive privacy in exchange for health services.	
	PS3	I feel comfortable disclosing highly sensitive privacy in exchange for health services.	
	PS4	I think it's safe to disclose highly sensitive privacy in exchange for health services.	
Highly sensitive privacy disclosure intention (PDI)	PDI1	I might be willing to let the system collect my highly sensitive privacy.	78
	PDI2	I might be willing to let the system collect my highly sensitive privacy.	
	PDI3	I am willing to let the system collect my highly sensitive privacy.	

professor and two research assistants) to review the scale, readability of the scale. The measurement scales for the revise and improve the semantics, coherence, and above seven variables are shown in Table 1.

In order to acquire authentic data while mitigating social desirability bias, a sequence of measures was undertaken during the construction of the survey questionnaire. Primarily, an anonymous online survey methodology was employed, accompanied by assurances of confidentiality to participants, thereby fostering an environment conducive to unreserved expression of real thoughts and sentiments. Additionally, meticulous attention was directed toward the formulation of questions, precluding explicit incorporation of specific societal expectations or assumptions to avert potential prompting of participants toward particular responses. Our survey consisted of multiple questions or options, and by randomizing their order, we reduced participants' sequence preferences or expectation biases, thereby increasing the objectivity of the data. Through the aforementioned strategies, we effectively addressed the potential challenge of social desirability bias prevalent in studies involving privacy disclosure, thereby ensuring the provision of candid and precise responses from the respondents.

To address the issue of nonresponse due to social desirability and fear of disclosure, we employed strategies to ensure anonymity and confidentiality, adhered to ethical principles, and provided explanations and background information. Firstly, we explicitly stated in the questionnaire that participants' responses would be treated confidentially and would not be associated with their personal identities. This helps to reduce concerns about social expectations and fear of disclosure, thus enhancing participants' comfort in answering sensitive questions. Secondly, we strictly adhered to ethical principles to ensure that survey questions do not cause psychological harm to participants while respecting their privacy rights and autonomy. Thirdly, we provided appropriate explanations and background information before addressing sensitive questions, explaining the reasons for collecting such sensitive information and the purpose of data collection. This helps to enhance participants' understanding and trust in the survey's objectives, thereby reducing fear of disclosure.

Data collection

In order to ensure the good reliability and validity of the questionnaire, this study first conducted a small-scale pre-survey, and then launched a large-scale questionnaire collection.

Presurvey. This study collected 40 sample data in the pre-survey, and the analysis results of the presurvey data showed that the reliability and validity of the questionnaire data were good. According to the feedback from the interviewees, this study conducted a further optimization and adjustment of the questionnaire topics, semantics, structure, and so on. For example, PV1 was changed from "I think

I will have a good experience" to "I think the system will bring me a good service experience" to make the question easier to understand. At the end of this study, a questionnaire on users' intention to disclose privacy in the HIHSS was formed, and a large-scale data collection was developed.

Formal collection. Starting from July 2022, this study began to formally collect data by distributing electronic questionnaires on the Internet. By August 2022, 250 samples have been collected. Before completing the questionnaire, every participant received an explanation regarding the study's objectives and aims, and subsequently, they provided a signed informed consent to participate in the research. In order to ensure the authenticity and reliability of the samples, this study checked and screened the results, and after eliminating the invalid questionnaires such as suspected duplicate questionnaire (the same IP address) and careless questionnaire (More than 80% of the items were the same option), 204 valid samples were obtained, with an effective rate of 81.6%. Table 2 shows the demographics of the sample. In all samples, 40.7% are male and 59.3% are female; 94.6% are aged 18 to 49,

Table 2. Demographic characteristics of the sample.

Construct	Item	Count	Percentage (%)
Gender	Male	83	40.7
	Female	121	59.3
Age	18 ~ 30 years old	130	63.7
	31 ~ 49 years old	63	30.9
	> 50 years old	11	5.4
Academic qualifications	High school and below	20	9.8
	Undergraduate/ Associate	142	69.6
	Graduate and above	42	20.6
Income	< 4500 yuan	96	47.1
	4500 ~ 8000 yuan	70	34.3
	> 8000 yuan	38	18.6
Privacy violation experience	Have	94	46.1
	None	110	53.9

and 5.4% are aged 50 and above; 9.8% of them have a high school education or below, and 90.2% of them have a bachelor's degree or above; 47.1% of them have a monthly income of less than 4500 yuan, and 52.9% of them have a monthly income of more than 4500 yuan; 46.1% of them have experienced privacy violation events, and 53.9% of them have not experienced privacy violation events.

Statistics analysis

All analyses were conducted with SPSS 25.0, MPLUS 7.0 and G*power. We conducted a prior power analysis to calculate the required sample size of the study with G*power V3.1.9.7. In this study, a conservative estimate was made by selecting an alpha error level of 0.05, recommended adequate power of 0.9 and medium effect size of 0.30.⁷⁹ Based on these criteria, it was determined that the minimum required sample size should not be below 109. Nonetheless, in order to guarantee a robust analysis, a substantial sample size of 204 participants was adopted.

To ensure the quality of the data, we conducted normality tests and multicollinearity tests on the data using SPSS. We find that the absolute values of kurtosis and skewness of all variables are less than 1, and most of the points in P-P diagram are scattered near the diagonal, so our data follows a normal distribution. The minimum VIF value of the independent variables is 1.811 and the maximum is 3.865. The VIF value is less than 10, and accordingly, there is no multicollinearity problem between independent variables.

Results

Common method biases test

After excluding invalid questionnaire, we conducted the tests of common method biases, reliability, and validity, and SEM on the remaining valid data using statistical analysis software SPSS 25.0 and MPLUS 7.0. In this study, "potential factor method of controlling the untested single method" was used to test common method biases. Firstly, conducting a confirmatory factor analysis model M1.

Table 3. Common method biases test.

Fit Index	M1	M2	M1-M2
χ^2/df	2.206	1.811	0.395
RMSEA	0.077	0.063	0.014
GFI	0.939	0.964	0.025
TLI	0.927	0.924	0.024

Secondly, conducting a model M2 containing methodological factors. The main fit metrics for Model M1 and Model M2 are shown in Table 3. The main fitting indexes of model M1 and model M2 are: $\Delta\chi^2/df=0.395$, $\Delta RMSEA=0.014$, $\Delta CFI=0.025$, and $\Delta TLI=0.024$. The change of each fitting index (M1-M2) is very small, indicating that the model has not been significantly improved after adding the common method factor, and there are no obvious common method biases in the measurement.⁸⁰

Measurement model checking

Test of fitting effect. Using confirmatory factor analysis to verify the fitting indicators of the measurement model. The results shows that $\chi^2/df=2.206<5$; $RMSEA=0.077<0$; $GFI=0.939>0.9$; $TLI=0.927>0.9$, which indicate the fitting effect of the measurement model is good.

Reliability test. Reliability refers to the extent to which the measurement scale of a variable is reliable, which is usually assessed by Cronbach's coefficient (CA), combined reliability (CR), and average variance extraction (AVE).⁸¹ It can be seen from Table 4 that the CA of each variable is between 0.776 and 0.925, which is greater than the minimum standard of 0.700;⁸² the CR is between 0.783 and 0.926, which is greater than the minimum standard of 0.600;⁸³ and the AVE is between 0.547 and 0.808, which is higher than the lowest standard of 0.500.⁸² Therefore, the scales used in this study have good reliability.

Convergent validity test. Convergent validity refers to the correlation between each measurement index of a specific variable in the measurement model, mainly tested by factor loading (FL).⁸² The results are shown in Table 4. The factor loadings of each variable in the questionnaire are between 0.698 and 0.914, which are greater than the minimum standard of 0.550.⁸⁴ Therefore, the scales used in this study have good convergent validity.

Discriminant validity test. Discriminant validity indicates the degree to which a variable differs from other variables. A variable has good discriminant validity if its correlation coefficient with all other variables is less than the square root of the AVE value of that variable.⁸⁵ It can be seen from Table 5 that the correlation coefficients of each variable with other variables are smaller than the diagonal data, i.e., the square root of AVE of each variable. Therefore, the scales used in this study have good discriminant validity.

Structural model test

Using SEM to test the model.⁸⁶ When employing SEM to assess relationships among variables through a

Table 4. Reliability test and convergent validity test.

Variables	Item	FL	AVE	CR	CA
PB	PB1	0.698	0.547	0.783	0.776
	PB2	0.736			
	PB3	0.782			
PVC	PVC1	0.899	0.789	0.918	0.915
	PVC2	0.914			
	PVC3	0.850			
PPT	PPT1	0.865	0.776	0.912	0.911
	PPT2	0.893			
	PPT3	0.884			
PR	PR1	0.752	0.703	0.904	0.903
	PR2	0.867			
	PR3	0.874			
	PR4	0.855			
PV	PV1	0.860	0.664	0.856	0.853
	PV2	0.760			
	PV3	0.822			
PS	PS1	0.845	0.733	0.917	0.915
	PS2	0.872			
	PS3	0.848			
	PS4	0.859			
PDI	PDI1	0.904	0.808	0.926	0.925
	PDI 2	0.903			
	PDI 3	0.889			

PB: perceived benefits; PPT: perceived effectiveness of privacy protection technologies; PVC: perceived justice of privacy violation compensation; PR: perceived risks; PV: perceived valence; PS: perceived security; PDI: privacy disclosure intention; FL: factor loading; AVE: average variance extraction; CA: Cronbach's alpha; CR: combined reliability.

measurement model, fundamental assumptions to consider encompass the reflective indicator assumption (i.e., where measurement variables reflect latent variables), endogeneity assumption (i.e., stating that relationships among latent

variables are determined by theoretical priors rather than measurement errors or external factors), the measurement error independence assumption, and so on. First, adopting four indicators to test the fitting effect of the structural model, and the results shows that $\chi^2/df = 1.980 < 5$; RMSEA = 0.069 < 0; GFI = 0.925 > 0.9; TLI = 0.914 > 0.9.⁸⁷ Four fitting indicators all meet the judgment criteria of the fitting degree index of the structural equation model, indicating that the fitting effect of the constructed structural equation model is good and a further test can be conducted.

Secondly, this study tests the path of structural equation model, and the test results are shown in Table 6 and Figure 2. In SEM, path coefficients are used to represent the relationships between latent variables. Path coefficients indicate the extent to which one latent variable influences another latent variable. The magnitude of the coefficient can be used to assess the strength of the relationship, where larger coefficients generally indicate stronger relationships. It can be seen that perceived valence ($\beta = 0.559$, $p < 0.001$) and perceived security ($\beta = 0.350$, $p < 0.01$) positively affect the disclosure intention of highly sensitive privacy, and H1 and H2 are supported. Perceived benefits positively affect perceived valence ($\beta = 0.367$, $p < 0.001$) and perceived security ($\beta = 0.192$, $p < 0.01$), and H3 and H4 are supported. Perceived risks negatively affect perceived valence ($\beta = -0.227$, $p = 0.01$) and perceived security ($\beta = -0.332$, $p < 0.001$), and H5 and H6 are supported. PJOPVC positively affects perceived valence ($\beta = 0.314$, $p < 0.001$) and perceived security ($\beta = 0.232$, $p < 0.01$), and H7 and H8 are supported. Perceived effectiveness of privacy protection technologies positively affects the perceived valence ($\beta = 0.184$, $p < 0.05$) and perceived security ($\beta = 0.279$, $p < 0.01$), and H9 and H10 are supported.

Finally, the study compares the path coefficients of H7 and H8, H9, and H10, and tests the hypotheses H11 and H12. The test results are shown in Table 7. The path coefficient between PJOPVC and perceived valence is larger than the path coefficient between PJOPVC and perceived security, the differential effect between path coefficients is larger ($\beta_{PVC \rightarrow PV} = 0.314 > \beta_{PVC \rightarrow PS} = 0.232$), H11 is supported. The path coefficient between PEOPTs and perceived valence is smaller than the path coefficient between PEOPTs and perceived security, and the differential effect between path coefficients is larger ($\beta_{PPT \rightarrow PV} = 0.184 < \beta_{PPT \rightarrow PS} = 0.279$), H12 is supported.

Mediating effect test

A bias-corrected nonparametric percentile Bootstrap method was used to test the mediating effects of perceived valence and perceived security, and test the validity of the model. The results are shown in Table 8. The magnitude of the effect value can reflect the strength of the indirect effect of the independent variable on the dependent variable

Table 5. Reliability test and convergent validity test.

Variables	Mean value	Standard deviation	PB	PVC	PPT	PR	PV	PS	PDI
PB	4.980	1.107	0.740						
PVC	3.897	1.519	0.466	0.888					
PPT	4.585	1.280	0.590	0.618	0.881				
PR	5.092	1.252	-0.448	-0.678	-0.653	0.838			
PV	4.616	1.151	0.635	0.681	0.696	0.659	0.815		
PS	4.225	1.279	0.549	0.698	0.727	-0.724	0.782	0.856	
PDI	4.201	1.508	0.549	0.703	0.709	-0.663	0.738	0.750	0.899

PB: perceived benefits; PPT: perceived effectiveness of privacy protection technologies; PVC: perceived justice of privacy violation compensation; PR: perceived risks; PV: perceived valence; PS: perceived security; PDI: privacy disclosure intention.

Table 6. Path coefficients and significance test.

Hypotheses	Path	Standardized coefficients	S.E.	C.R.	<i>p</i>	Result
H1	PV→PDI	0.559	0.112	4.999	0.000***	Accept
H2	PS→PDI	0.350	0.113	3.085	0.002**	Accept
H3	PB→PV	0.367	0.076	4.862	0.000***	Accept
H4	PB→PS	0.192	0.073	2.643	0.008**	Accept
H5	PR→PV	-0.227	0.081	-2.784	0.005**	Accept
H6	PR→PS	-0.332	0.079	-4.218	0.000***	Accept
H7	PVC→PV	0.314	0.074	4.254	0.000***	Accept
H8	PVC→PS	0.232	0.072	3.239	0.001**	Accept
H9	PPT→PV	0.184	0.092	2.004	0.045*	Accept
H10	PPT→PS	0.279	0.087	3.194	0.001**	Accept

PB: perceived benefits; PPT: perceived effectiveness of privacy protection technologies; PVC: perceived justice of privacy violation compensation; PR: perceived risks; PV: perceived valence; PS: perceived security; PDI: privacy disclosure intention.

Note: *p* * < 0.05, *p* ** < 0.01, *p* *** < 0.001, same as below.

through the mediating variable. If the interval [BootLLCI, BootULCI] does not include 0, then the mediating effect is statistically significant. Perceived valence (effect = 0.292; 95% CI = 0.171 ~ 0.435) and perceived security (effect = 0.323; 95% CI = 0.170 ~ 0.464) have significant mediating effects on perceived benefits and the willingness to disclose highly sensitive privacy. Perceived valence (effect = 0.199; 95% CI = 0.106 ~ 0.293) and perceived

security (effect = 0.228; 95% CI = 0.066 ~ 0.390) have significant mediating effects on perceived justice of privacy violence compensation and the disclosure intention of highly sensitive privacy. Perceived valence (effect = 0.248; 95% CI = 0.136 ~ 0.378) and perceived security (effect = 0.274; 95% CI = 0.097 ~ 0.446) have significant mediating effects on the PEOPTs and the disclosure intention of highly sensitive privacy. Perceived valence

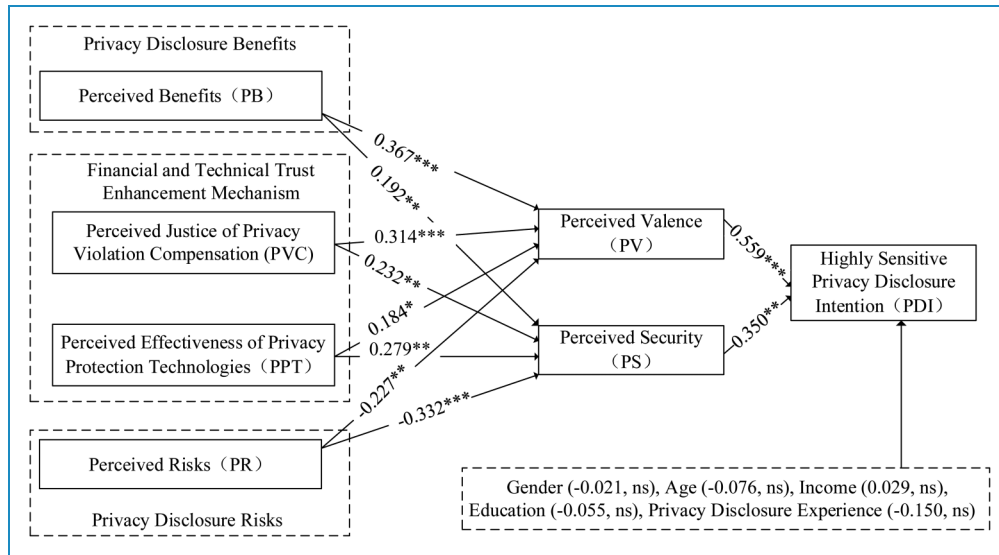


Figure 2. Path coefficient and significance.

Table 7. Comparison of path coefficient.

Hypotheses	Path	Standardized Coefficients	S.E.	$t_{spooled}$ ($ t_{spooled} > 0.8$) ⁸⁸	Result
H11	PVC→PV(H7)	0.314	0.074	11.344	Accept
	PVC→PS(H8)	0.232	0.072		
H12	PPT→PV(H9)	0.184	0.092	-10.716	Accept
	PPT→PS(H10)	0.279	0.087		

PPT: perceived effectiveness of privacy protection technologies; PVC: perceived justice of privacy violation compensation; PV: perceived valence; PS: perceived security.

Table 8. Mediating effects test of perceived valence and perceived security.

Path	Effect	S.E.	BootLLCI	BootULCI	Result
PB→PV→PDI	0.292	0.067	0.171	0.435	Remarkable
PB→PS→PDI	0.323	0.075	0.170	0.464	Remarkable
PVC→PV→PDI	0.199	0.047	0.106	0.293	Remarkable
PVC→PS→PDI	0.228	0.084	0.066	0.390	Remarkable
PPT→PV→PDI	0.248	0.060	0.136	0.378	Remarkable
PPT→PS→PDI	0.274	0.088	0.097	0.446	Remarkable
PR→PV→PDI	-0.274	0.053	-0.380	-0.173	Remarkable
PR→PS→PDI	-0.301	0.087	-0.461	-0.122	Remarkable

PB: perceived benefits; PPT: perceived effectiveness of privacy protection technologies; PVC: perceived justice of privacy violation compensation; PR: perceived risks; PV: perceived valence; PS: perceived security; PDI: privacy disclosure intention.

(effect = -0.274 ; 95% CI = $-0.380 \sim -0.173$) and perceived security (effect = -0.301 ; 95% CI = $-0.461 \sim -0.122$) have significant mediating effects on perceived risks and the disclosure intention of highly sensitive privacy.

Discussion

Research findings

This study has the following three key findings. First, perceived benefits and perceived risks are important determinants of perceived valence and perceived security (H3, H4, H5, H6), which further affect users' willingness to disclose highly sensitive privacy to the HIHSS (H1, H2). On the one hand, if users believe that disclosing highly sensitive privacy to the HIHSS can bring them beneficial health services, their perceived valence and perceived security will be enhanced, which in turn promotes their disclosure of highly sensitive privacy to the HIHSS. On the other hand, the disclosure of highly sensitive privacy to the HIHSS often involves the potential risk of privacy disclosure, which will cause the reduction of perceived valence and perceived security, thus inhibiting users from disclosing highly sensitive privacy to the HIHSS.

Secondly, the study shows perceived justice of privacy violation compensation and PEOPTs have a common effect, both of which promote users to disclose highly sensitive privacy to the HIHSS by establishing good perceived valence and perceived security (H7, H8, H9, H10). Previous studies have explored the effects of privacy violation compensation and privacy protection technologies on users' behavioral intentions. For example, Hazarika et al.⁶⁶ have studied the impact of privacy violation compensation on users' repurchase intention. Frey et al.⁸⁹ have studied the impact of block chain technologies on users' willingness to disclose privacy. This study integrates these two types of studies and confirms the common effect of PJOPVC and PEOPTs on users' willingness to disclose highly sensitive privacy in HIHSS.

Finally, PJOPVC and PEOPTs have differential effects in improving users' willingness to disclose highly sensitive privacy to the HIHSS (H11, H12). Specifically, PJOPVC has a greater impact on the perceived valence, while PEOPTs has a greater impact on the perceived security. In existing research, the differential effect of financial trust enhancement mechanism and technical trust enhancement mechanism is largely ignored. According to trust-related studies,^{37,73} privacy violation compensation is highly related to the user's good-will-centered response while privacy protection technologies are highly related to the user's ability-centered response. Good-will-centered coping style can effectively reduce the user's expectation of loss caused by privacy violation events, so it has a greater impact on the formation of perceived valence than perceived security. Ability-centered coping style is

helpful for users to produce good emotions to cope with risk situations, so it plays a more important role in the formation of perceived security than perceived valence.

Contribution

The theoretical contributions of this study are as follows. First of all, this study applies the privacy calculus theory to explain the user's HSPDI in the HIHSS, which broadens the application scope of the privacy calculus theory. Privacy calculus theory has been widely used in the study of users' privacy-related behaviors in the field of health services. However, the existing studies mainly focus on users' privacy-related behaviors in electronic health record system,^{90,91} online health communities,^{30,92,93} mobile health applications,^{94,95} and other systems, and there are few studies related to HIHSSs. As a new health service model, home intelligent health service model enables users to enjoy intelligent and personalized medical or nursing services in the home environment, but at the same time, it also raises more serious privacy concerns as it relies on the collection of highly sensitive private information from users. Our empirical results show privacy calculus also exists in the process of user's highly sensitive privacy disclosure decisions in the HIHSS. Secondly, this study explores the common and differential effects of financial trust enhancement mechanism and technical trust enhancement mechanism on users' HSPDI in HIHSS, enriching the research on information privacy. Although previous privacy-related studies have recognized the importance of financial and technical trust enhancement mechanisms,^{21,22} not much attention has been paid to how exactly these two mechanisms affect users' willingness to disclose their privacy. This study makes up for the lack of research by examining the common and differential effects of these two trust enhancement mechanisms on users' willingness to disclose highly sensitive privacy in HIHSS.

On the practical side, firstly, the common effect suggests service providers should focus on financial trust enhancement mechanism and technical trust enhancement mechanism when managing highly sensitive privacy disclosure of users in HIHSSs. On the one hand, home intelligent health service providers should investigate the scope of users' demand for privacy violation compensation, make fair financial compensation commitments to users, and enhance users' trust. On the other hand, it is suggested that home intelligent service providers adopt effective privacy protection technologies to prevent the leakage of user privacy information, such as block chain technologies, edge computing technologies, etc. At the same time, home intelligent health service providers need to popularize privacy protection technologies for users, increase users' understanding of privacy protection technologies, and enhance users' perception of the effectiveness of technologies. Secondly, the differential effect suggests home

intelligent health service providers should strategically utilize financial trust enhancement mechanism and technical trust enhancement mechanism to facilitate users' highly sensitive privacy disclosure in HIHSS. Specifically, the PJOPVC mainly affects the formation of perceived valence to affect the user's willingness to disclose highly sensitive privacy while the privacy protection technologies mainly improve users' perceived security to enhance the users' willingness to disclose highly sensitive privacy. Therefore, it is recommended that home intelligent health service providers evaluate users' perceived valence and perceived security for highly sensitive privacy disclosure, and adopt different trust enhancement mechanisms for different types of users. For the users with low perceived valence level, it is more effective to improve their highly sensitive privacy disclosure willingness by improving the fairness of privacy violation compensation. For users with low perceived security, their willingness to disclose highly sensitive privacy can be improved by enhancing the effectiveness of privacy protection technologies.

The PJOPVC can characterize fairness and accountability in a trust-enhancing environment. The PEOPTs can characterize consumer protection in a trust-enhancing environment. Based on these two concepts, evaluation criteria can be designed for regulatory policies and regulations, to review the regulatory policies and regulations of HIHSSs, ensuring that they encompass the core requirements of fairness, accountability, and consumer protection. This includes provisions on accessing and using personal health data, data security, privacy protection requirements, and so on.

Limitations and future research

There are some shortcomings in this study which are expected to be improved in future studies. For instance, this study only explored the mechanisms influencing users' intention to disclose privacy in the HIHSS, without examining the actual behavior of users. Behavioral intention is a crucial driving force behind behavior, and the relationship between behavioral intention and behavior can be considered as a causal relationship, implying that individuals or systems must have a clear intention or goal before engaging in the behavior. Behavior itself represents the actualization process of the behavioral intention, as it transforms the intention into concrete actions. However, there may be a gap between behavioral intention and actual behavior, and a high intention to disclose privacy does not necessarily mean that users will agree to disclose privacy. In future research, users' actual behavior to disclose privacy in community health service systems can be modeled and studied.

Conclusion

In conclusion, by expanding upon the privacy calculus theory and considering the impact of service providers'

trust enhancement mechanisms, the study has revealed the intricate relationship between perceived benefits, perceived risks, perceived valence, and perceived security, and how these factors collectively influence users' decisions regarding highly sensitive privacy disclosure. Our findings underscore the significance of perceived benefits and perceived risks as potent determinants of perceived valence and perceived security. These factors, in turn, exert a substantial influence on users' HSPDIs. Notably, we have identified that PJOPVC holds greater sway over perceived valence while the PEOPTs exerts a more pronounced impact on perceived security. Overall, this study contributes valuable insights to the field of privacy management in the context of intelligent health services and offers practical recommendations for service providers and policymakers seeking to establish trust and facilitate informed privacy-related decisions among users.

Acknowledgments: We would like to express our gratitude and appreciation to all those participants who gave us the possibility to complete this study.

Declaration of conflicting interests: The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding: The authors disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by the National Natural Science Foundation of China (Nos 71871135 and 72271155).

Guarantor: F Liu and YF Wei.

Contributorship: F Liu and YF Wei visualized, reviewed, and edited the study. SG Li conceived the study and contributed to funding acquisition, project administration, validation, and supervision. RX Li was involved in formal analysis, software operation, and validation. BY Zhu contributed to methodology and validation. BY Zhang conceptualized the study and wrote the first draft of the manuscript. JY Li contributed to resources and investigation. All authors reviewed and edited the manuscript and approved the final version of the manuscript.

ORCID iD: Ruoxuan Li  <https://orcid.org/0009-0000-6959-2866>

Supplemental material: Supplemental material for this article is available online.

References

1. Xiang X and Wang Y. Current situation, characteristics, causes and countermeasures of population aging in China. *Chin J Gerontol* 2021; 41: 4149–4152.

2. Shi D, Zhang K and Xu B. Development of cloud intelligent real-time fall detection system for the aged population. *Comput Eng Applic* 2016; 52: 259–264.
3. Srivastava G, Dwivedi AD and Singh R. Automated remote patient monitoring: Data sharing and privacy using blockchain. *arXiv preprint arXiv:181103417* 2018.
4. STATISTA. Ethical concerns surrounding AI technology use in healthcare in the United States as of 2021, “<https://www.statista.com/statistics/1256727/ethical-concerns-about-ai-in-healthcare-in-the-us/>” (2021, accessed 23 November 2022).
5. Anderson JG. Social, ethical and legal barriers to e-health. *Int J Med Inf* 2007; 76: 480–483.
6. Fernández-Alemán JL, Señor IC, Lozoya PÁO, et al. Security and privacy in electronic health records: a systematic literature review. *J Biomed Inform* 2013; 46: 541–562.
7. Elhoseny M, Thilakarathne NN, Alghamdi MI, et al. Security and privacy issues in medical internet of things: overview, countermeasures, challenges and future directions. *Sustainability* 2021; 13: 11645.
8. Almalawi A, Khan AI, Alsolami F, et al. Managing security of healthcare data for a modern healthcare system. *Sensors* 2023; 23: 3612.
9. Yang Q, Gong X, Zhang KZ, et al. Self-disclosure in mobile payment applications: common and differential effects of personal and proxy control enhancing mechanisms. *Int J Inf Manage* 2020; 52: 102065.
10. Wang Y. Research on the influencing factors of Users’ health information disclosure intention in online medical community. *Journal of Information Resources Management* 2018; 8: 93–103, cover 03.
11. Zhou J. Factors influencing people’s personal information disclosure behaviors in online health communities: a pilot study. *Asia Pacific Journal of Public Health* 2018; 30: 286–295.
12. Laufer RS and Wolfe M. Privacy as a concept and a social issue: a multidimensional developmental theory. *Journal of Social Issues* 1977; 33: 22–42.
13. Smith HJ, Dinev T and Xu H. Information privacy research: an interdisciplinary review. *MIS Q* 2011; 35: 989–1015.
14. Rahaman A, Islam MM, Islam MR, et al. Developing IoT based smart health monitoring systems: a review. *Rev D’Intelligence Artif* 2019; 33: 435–440.
15. Lapolla P and Lee R. Privacy versus safety in contact-tracing apps for coronavirus disease 2019. *DIGITAL HEALTH* 2020; 6: 2055207620941673.
16. Malhotra NK, Kim SS and Agarwal J. Internet users’ information privacy concerns (IUIPC): the construct, the scale, and a causal model. *Inf Syst Res* 2004; 15: 336–355.
17. Bol N, Dienlin T, Kruike-meier S, et al. Understanding the effects of personalization as a privacy calculus: analyzing self-disclosure across health, news, and commerce contexts. *J Comput Mediat Commun* 2018; 23: 370–388.
18. Leon S, Chen C and Ratcliffe A. Consumers’ perceptions of last mile drone delivery. *Int J Logist Res* 2023; 26: 345–364.
19. Chellappa RK and Pavlou PA. Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logist Inf Manage* 2002; 15: 358–368.
20. Wang L, Sun Z, Dai X, et al. Retaining users after privacy invasions: the roles of institutional privacy assurances and threat-coping appraisal in mitigating privacy concerns. *Inf Technol People* 2019; 32: 1679–1703.
21. Choi BC, Kim SS and Jiang Z. Influence of firm’s recovery endeavors upon privacy breach on online customer behavior. *J Manage Inf Syst* 2016; 33: 904–933.
22. Sun Y, Fang S and Hwang Y. Investigating privacy and information disclosure behavior in social electronic commerce. *Sustainability* 2019; 11: 3311.
23. Hallam C and Zanella G. Online self-disclosure: the privacy paradox explained as a temporally discounted balance between concerns and rewards. *Comput Human Behav* 2017; 68: 217–227.
24. Wang L, Yan J, Lin J, et al. Let the users tell the truth: self-disclosure intention and self-disclosure honesty in mobile social networking. *Int J Inf Manage* 2017; 37: 1428–1440.
25. Chen H-T. Revisiting the privacy paradox on social media with an extended privacy calculus model: the effect of privacy concerns, privacy self-efficacy, and social capital on privacy management. *American Behavioral Scientist* 2018; 62: 1392–1412.
26. Kim B and Kim D. Understanding the key antecedents of users’ disclosing behaviors on social networking sites: the privacy paradox. *Sustainability* 2020; 12: 5163.
27. Keith MJ, Babb J, Furner C, et al. Limited information and quick decisions: consumer privacy calculus for mobile applications. *AIS Transactions on Human-Computer Interaction (THCI)* 2016; 8: 88–130.
28. Nguyen HM and Khoa BT. The relationship between the perceived mental benefits, online trust, and personal information disclosure in online shopping. *The Journal of Asian Finance, Economics and Business* 2019; 6: 261–270.
29. Dienlin T and Metzger MJ. An extended privacy calculus model for SNSs: analyzing self-disclosure and self-withdrawal in a representative US sample. *J Comput Mediat Commun* 2016; 21: 368–383.
30. Zhang X, Liu S, Chen X, et al. Health information privacy concerns, antecedents, and information disclosure intention in online health communities. *Information & Management* 2018; 55: 482–493.
31. Weiwei L, Xu Z and Meng Z. Study on influencing factors of privacy disclosure behavior of online health communities users. *Journal of Medical Information* 2022; 35: 5–9.
32. Krasnova H, Günther O, Spiekermann S, et al. Privacy concerns and identity in online social networks. *Identity in the Information Society* 2009; 2: 39–63.
33. Bansal G and Zahedi FM. Trust-discount tradeoff in three contexts: frugality moderating privacy and security concerns. *J Comput Inf Syst* 2014; 55: 13–29.
34. Liu X, He X, Wang M, et al. What influences patients’ continuance intention to use AI-powered service robots at hospitals? The role of individual characteristics. *Technol Soc* 2022; 70: 101996.
35. Li H, Wu J, Gao Y, et al. Examining individuals’ adoption of healthcare wearable devices: an empirical study from privacy calculus perspective. *Int J Med Inf* 2016; 88: 8–17.
36. Lui SS and Ngo H-Y. The role of trust and contractual safeguards on cooperation in non-equity alliances. *J Manage* 2004; 30: 471–485.
37. Mayer RC, Davis JH and Schoorman FD. An integrative model of organizational trust. *Acad Manage Rev* 1995; 20: 709–734.

38. McAllister DJ. Affect-and cognition-based trust as foundations for interpersonal cooperation in organizations. *Acad Manage J* 1995; 38: 24–59.
39. Barber B. The logic and limits of trust. *Contemp Sociol* 1983; 13: 384.
40. Johnston AM, Mills CM and Landrum AR. How do children weigh competence and benevolence when deciding whom to trust? *Cognition* 2015; 144: 76–90.
41. Levin DZ and Cross R. The strength of weak ties you can trust: the mediating role of trust in effective knowledge transfer. *Manage Sci* 2004; 50: 1477–1490.
42. Athos AG and Gabarro JJ. *Interpersonal behavior: communication and understanding in relationships*. 1st ed. Englewood Cliffs, NJ: Prentice Hall, 1978, pp.290–303.
43. Nooteboom B. Trust, opportunism and governance: a process and control model. *Organization Studies* 1996; 17: 985–1010.
44. Phelps J, Nowak G and Ferrell E. Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing* 2000; 19: 27–41.
45. Stewart KA and Segars AH. An empirical examination of the concern for information privacy instrument. *Inf Syst Res* 2002; 13: 36–49.
46. Brady MK and Cronin Jr JJ. Some new thoughts on conceptualizing perceived service quality: a hierarchical approach. *J Mark* 2001; 65: 34–49.
47. Kavya TS, Jang Y-M, Tsogtbaatar E, et al. Fall detection system for elderly people using vision-based analysis. *Sci Technol* 2020; 23: 69–83.
48. Harrou F, Zerrouki N, Sun Y, et al. An integrated vision-based approach for efficient human fall detection in a home environment. *IEEE Access* 2019; 7: 114966–114974.
49. Panahi L and Ghods V. Human fall detection using machine vision techniques on RGB–D images. *Biomed Signal Process Control* 2018; 44: 146–153.
50. King C-H, Chen TL, Jain A, et al. Towards an assistive robot that autonomously performs bed baths for patient hygiene. In: 2010 *IEEE/RSJ International Conference on Intelligent Robots and Systems* 2010, pp.319–324. IEEE.
51. Zhang F, Cully A and Demiris Y. Probabilistic real-time user posture tracking for personalized robot-assisted dressing. *IEEE Trans Robot* 2019; 35: 873–888.
52. Chance G, Jevtić A, Caleb-Solly P, et al. “Elbows out”—predictive tracking of partially occluded pose for robot-assisted dressing. *IEEE Robotics and Automation Letters* 2018; 3: 3598–3605.
53. Akalin N, Kristoffersson A and Loutfi A. Evaluating the sense of safety and security in human–robot interaction with older people. In: Korn O (ed) *Social robots: technological, societal and ethical aspects of human-robot interaction*. 1st ed. Cham, Switzerland: Springer Cham, 2019, pp.237–264.
54. Dinev T, McConnell AR and Smith HJ. Research commentary—informing privacy research through information systems, psychology, and behavioral economics: thinking outside the “APCO” box. *Inf Syst Res* 2015; 26: 639–655.
55. Liu J, Xia Y and Tang Z. Privacy-preserving video fall detection using visual shielding information. *Vis Comput* 2021; 37: 359–370.
56. Bursleson W, Lozano C, Ravishankar V, et al. An assistive technology system that provides personalized dressing support for people living with dementia: capability study. *JMIR Med Inform* 2018; 6: e5587.
57. Nguyen TT, Tran Hoang MT and Phung MT. “To our health!” perceived benefits offset privacy concerns in using national contact-tracing apps. *Libr Hi Tech* 2022; 41: 174–191.
58. Schomakers E-M, Lidynia C and Ziefle M. The role of privacy in the acceptance of smart technologies: applying the privacy calculus to technology acceptance. *International Journal of Human–Computer Interaction* 2022; 38: 1276–1289.
59. Xu H, Dinev T, Smith J, et al. Information privacy concerns: linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems* 2011; 12: 1.
60. Xu H, Luo XR, Carroll JM, et al. The personalization privacy paradox: an exploratory study of decision making process for location-aware marketing. *Decis Support Syst* 2011; 51: 42–52.
61. Woogara J. Patients’ privacy of the person and human rights. *Nurs Ethics* 2005; 12: 273–287.
62. Malaquias RF and Hwang Y. An empirical study on trust in mobile banking: a developing country perspective. *Comput Human Behav* 2016; 54: 453–461.
63. Dinev T, Xu H, Smith JH, et al. Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *Eur J Inf Syst* 2013; 22: 295–316.
64. Li H, Sarathy R and Xu H. The role of affect and cognition on online consumers’ decision to disclose personal information to unfamiliar online vendors. *Decis Support Syst* 2011; 51: 434–445.
65. Xu H, Teo H-H, Tan BC, et al. The role of push-pull technology in privacy calculus: the case of location-based services. *J Manage Inf Syst* 2009; 26: 135–174.
66. Hazarika BB, Gerlach J and Cunningham L. The role of service recovery in online privacy violation. *International Journal of E-Business Research (IJEER)* 2018; 14: 1–27.
67. Hann I-H, Hui K-L, Lee S-YT, et al. Overcoming online information privacy concerns: an information-processing theory approach. *J Manage Inf Syst* 2007; 24: 13–42.
68. Shin H, Ryu K, Kim J-Y, et al. Application of privacy protection technology to healthcare big data. *Res Sq* ahead of print 12 September 2022. DOI: 10.21203/rs.3.rs-2035438/v1
69. Popp R and Poindexter J. Countering terrorism through information and privacy protection technologies. *IEEE Secur Priv* 2006; 4: 18–27.
70. Ramyasri G and Hussain SJ. Access Control of Healthcare Data using Blockchain Technology. In: 2021 *2nd International Conference on Smart Electronics and Communication (ICOSEC)* 2021, pp.353-357. IEEE.
71. Xu H. The effects of self-construal and perceived control on privacy concerns. In: *Proceedings of the International Conference on Information Systems Canada: Montreal, 9-12 December 2007* 2007.
72. Di Battista S, Pivetti M and Berti C. Competence and benevolence as dimensions of trust: lecturers’ trustworthiness in the words of Italian students. *Behavioral Sciences* 2020; 10: 143.
73. Milne GR and Rohm AJ. Consumer privacy and name removal across direct marketing channels: exploring opt-in and opt-out alternatives. *Journal of Public Policy & Marketing* 2000; 19: 238–249.

74. Culnan MJ. Protecting privacy online: is self-regulation working? *Journal of Public Policy & Marketing* 2000; 19: 20–26.
 75. Webster J and Trevino LK. Rational and social theories as complementary explanations of communication media choices: two policy-capturing studies. *Acad Manage J* 1995; 38: 1544–1572.
 76. Kim D, Park K, Park Y, et al. Willingness to provide personal information: perspective of privacy calculus in IoT services. *Comput Human Behav* 2019; 92: 273–281.
 77. Bartneck C, Kulić D, Croft E, et al. Measuring instruments for the anthropomorphism, animacy, likeability, perceived intelligence and perceived safety of robots. *Int J Soc Robot* 2009; 1: 71–81.
 78. Sun Y, Wang N, Shen X-L, et al. Location information disclosure in location-based social network services: privacy calculus, benefit structure, and gender differences. *Comput Human Behav* 2015; 52: 278–292.
 79. Cohen J. A power primer. *Psychol Bull* 1992; 112: 155–159.
 80. Xiong H-X, Zhang J, Ye B-J, et al. Common method variance effects and the models of statistical approaches for controlling it. *Advances in Psychological Science* 2012; 20: 757.
 81. Anderson JC and Gerbing DW. Structural equation modeling in practice: a review and recommended two-step approach. *Psychol Bull* 1988; 103: 11.
 82. Nunnally JC and Ih B. *Psychometric theory*. 3rd ed. New York, USA: McGraw-Hill, 1994.
 83. Bagozzi RP and Yi Y. On the evaluation of structural equation models. *Journal of the Academy of Marketing Science* 1988; 16: 74–94.
 84. Tabachnick BG, Fidell LS and Ullman JB. *Using multivariate statistics*. 5th ed. Boston, MA: Pearson, 2006.
 85. Fornell C and Larcker DF. Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research* 1981; 18: 39–50.
 86. Chen K. Characteristics and applications of structural equation modelling. *Statistics & Decision* 2006; 10: 22–25. DOI:10.13546/j.cnki.tjyj.2006.10.008.
 87. McDonald RP and Ho M-HR. Principles and practice in reporting structural equation analyses. *Psychol Methods* 2002; 7: 64.
 88. Zheng H, Wen Z and Wu Y. The appropriate effect sizes and their calculations in psychological research. *Adv Cogn Psychol* 2011; 19: 1868–1878.
 89. Frey RM, Bühler P, Gerdes A, et al. The effect of a blockchain-supported, privacy-preserving system on disclosure of personal data. In: 2017 *IEEE 16th International Symposium on Network Computing and Applications (NCA)* 2017, pp.1-5. IEEE.
 90. Cherif E, Bezaz N and Mzoughi M. Do personal health concerns and trust in healthcare providers mitigate privacy concerns? Effects on patients' intention to share personal health data on electronic health records. *Soc Sci Med* 2021; 283: 114146.
 91. Li H, Gupta A, Zhang J, et al. Examining the decision to use standalone personal health record systems as a trust-enabled fair social contract. *Decis Support Syst* 2014; 57: 376–386.
 92. Yuchao W, Ying Z and Liao Z. Health privacy information self-disclosure in online health community. *Front Public Health* 2021; 8: 602792.
 93. Kordzadeh N, Warren J and Seifi A. Antecedents of privacy calculus components in virtual health communities. *Int J Inf Manage* 2016; 36: 724–734.
 94. Fox G, Clohessy T, van der Werff L, et al. Exploring the competing influences of privacy concerns and positive beliefs on citizen acceptance of contact tracing mobile applications. *Comput Human Behav* 2021; 121: 106806.
 95. Tran CD and Nguyen TT. Health vs. privacy? The risk-risk tradeoff in using COVID-19 contact-tracing apps. *Technol Soc* 2021; 67: 101755.
-