International Journal of Medical Informatics 88 (2016) 8–17

Contents lists available at ScienceDirect

International Journal of Medical Informatics

journal homepage: www.ijmijournal.com

Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective

He Li[a,b], Jing Wu[b,*], Yiwen Gao[b], Yao Shi[a]

[a] Fogelman College of Business and Economics, The University of Memphis, United States
[b] School of Economic Information Engineering, Southwestern University of Finance and Economics, China

ARTICLE INFO

Article history:
Received 1 March 2015
Received in revised form 9 December 2015
Accepted 13 December 2015

Keywords:
Wearable devices
Healthcare
Adoption
Privacy calculus

ABSTRACT

Background: Wearable technology has shown the potential of improving healthcare efficiency and reducing healthcare cost. Different from pioneering studies on healthcare wearable devices from technical perspective, this paper explores the predictors of individuals' adoption of healthcare wearable devices. Considering the importance of individuals' privacy perceptions in healthcare wearable devices adoption, this study proposes a model based on the privacy calculus theory to investigate how individuals adopt healthcare wearable devices.
Method: The proposed conceptual model was empirically tested by using data collected from a survey. The sample covers 333 actual users of healthcare wearable devices. Structural equation modeling (SEM) method was employed to estimate the significance of the path coefficients.
Results: This study reveals several main findings: (1) individuals' decisions to adopt healthcare wearable devices are determined by their risk–benefit analyses (refer to privacy calculus). In short, if an individual's perceived benefit is higher than perceived privacy risk, s/he is more likely to adopt the device. Otherwise, the device would not be adopted; (2) individuals' perceived privacy risk is formed by health information sensitivity, personal innovativeness, legislative protection, and perceived prestige; and (3) individuals' perceived benefit is determined by perceived informativeness and functional congruence. The theoretical and practical implications, limitations, and future research directions are then discussed.

1. Introduction

Wearable device, the new electronic technology with accessory and sensor features, has shown its value in various fields. The emergence of wearable device provides more opportunities for back-end players (i.e., startups and App developers) and big data analytics initiatives [1]. Specially, depending on wearable device's unique advantage on tracking and transforming users' health information in real-time [2], it has been widely adopted in the healthcare sector. Up to now, there are two main kinds of healthcare wearable devices in the market, fitness and medical wearable devices. By adopting a proper fitness wearable device such as Fitbit Flex and Jawbone UP, users can monitor their health conditions such as sleep, calories burned, heart rate, and distance traveled in real time. Unfortunately, managing serious diseases requires more than just tracking these physical parameters. To this end, some innovative firms such as Google and Apple are making efforts on researching medical wearable devices. Users not only could monitor their fitness parameters, but also may receive personalized medical suggestions and get their physical information such as blood pressure, oxygen level, and gene expression. In this paper, our definition of healthcare wearable devices includes both, fitness and medical wearable devices.

According to the recent report released by P&S Market Research,[1] the global healthcare wearable device (that includes fitness and medical wearable devices) market was valued at 157 million dollars in 2014, and it is predicted to reach 1630.3 million dollars by 2020 with a growth rate of 46.6% during the years 2015–2020. Thus, wearable devices have the huge potential development in the future. However, a report from PricewaterhouseCoopers' Health Research Initiative (HRI) in 2014 notes that almost one third users who own a wearable device use it on a daily basis, while the privacy is one of the key apprehensions of consumers. 82% of respondents was worried about that wearable

* Corresponding author at: No. 555 Liutai Ave, Wenjiang District, Chengdu 611130, China.
E-mail addresses: kaitlynwu@swufe.edu.cn, kaitlynwu@gmail.com (J. Wu).

[1] http://news.sys-con.com/node/3387418.

http://dx.doi.org/10.1016/j.ijmedinf.2015.12.010
1386-5056/

Table 1
Prior studies about HIT adoption.

Literature	HIT type	Theory	Main factors
[25]	EHR	ELM	Privacy concern, argument frame, issue involvement
[10]	MHS	TAM	Perceived usefulness, perceived ease of use, subjective norm, output quality, result demonstrability
[24]	PHR	PBT	Privacy concern, trust, emotion, information type, intended purpose
[26]	EHR, PHR	Game theory	Switching cost
[28]	MHS	TAM	Perceived usefulness, perceived ease of use, self-efficacy, technology anxiety
[11]	HIT	TAM	Compatibility, information quality, perceived ease of use, perceived usefulness
[31]	Ubiquitous HIT	TAM	Perceived ease of use, perceived usefulness, perceived enjoyment
[27]	EHR	IDT	Identity reinforcement, identity deterioration, government influence
[29]	MHS	TAM, TPB	Perceived ease of use, perceived usefulness, personal innovativeness, perceived behavioral control, subjective norm, perceived service availability
[9]	Biometrics	TAM, DOI, UTAUT, PCT	Perceived ease of use, perceived usefulness, compatibility, trust, privacy concern, perceived risk, social influence, facilitating condition
[30]	Clinical DSS	TAM	Perceived ease of use, computer knowledge, general optimism
[33]	HIT	TAM, TPB	Perceived usefulness, compatibility, trust, co-worker's viewpoints
[32]	MHS	DFM, TAM	Perceived ease of use, perceived usefulness, technology anxiety, resistance to change
[15]	PHR	PCT, SCT	Perceived benefit, trust belief, perceived privacy risk, privacy control
[12]	MHS	TAM, TPB, UTAUT, PMT	Response efficacy, perceived ease of use, subjective norm, response cost, self-efficacy, perceived vulnerability, perceived severity
[34]	MHS	TPB	Perceived value, perceived behavioral control, subjective norm, gender difference, attitude
This study	Healthcare wearable technology	PCT	Health information sensitivity, personal innovativeness, legislative protection, perceived prestige, perceived informativeness, functional congruence

devices would invade their privacy.[2] In addition, to make full use of wearable devices in shaping new health economy, it would be essential to address consumer's concerns such as privacy and cost. Therefore, from industrial aspect, there is urgent demand to study the privacy issue of healthcare wearable devices.

To date, most extant studies about healthcare wearable devices have focused on the technical perspective. They have made continuous efforts on exploring new technology that can be applied in healthcare sector (e.g., Refs. [3,4]) and developing specific healthcare wearable devices (e.g., Refs. [5–8]). Although the perception and responses of end users are quite important for designers to develop better devices [9], the research on empirically examining individuals' behaviors such as adoption intention toward healthcare wearable devices is sparse. By conducting a literature study of prior health information technology (HIT) adoption research, we found that most extant related studies investigate individuals' adoption toward HIT from technology and healthcare behavior perspectives (e.g., Refs. [10–12]). Although privacy issue plays a critical role in determining individuals' intention to adopt HIT due to the higher sensitivity of health information [13,14], only a few studies have considered the factors related to privacy perception as independent variables and without any further investigation of privacy perception formation [9,15]. According to the above analysis, we are going to empirically investigate the factors that would affect individuals' adoption of healthcare wearable devices from privacy calculus perspective, since users' decisions to use healthcare wearable devices are affected by their risk–benefit analyses [9,15–17]. In addition, we also examine several important antecedent factors of individuals' privacy calculus for healthcare wearable devices adoption. In detail, we hypothesize the effects of health information sensitivity, personal innovativeness in IT, legislative protection, perceived prestige, and perceived informativeness on individuals' perceived privacy risk. The impacts of perceived informativeness and functional congruence on individuals' perceived benefits are also predicted.

The proposed conceptual model was tested by adopting the structural equation modeling (SEM) method to analyze the empirical data collected from 333 respondents. Most hypotheses proposed in our model were validated in the data. This study provides several implications for both theory and practice. From a theoretical perspective, to the best of our knowledge, we are among the first to empirically test the predictors of individuals' adoption of healthcare wearable devices, which is quite different from pioneering healthcare wearable devices studies from technical perspective [3–8]. In addition, by exploring the adoption of an understudied and emerging HIT—healthcare wearable device from privacy calculus perspective, this research contributes to prior literature about HIT adoption from technology and healthcare perspective [10–12]. From a practical perspective, business managers are guided to conduct better marketing strategies, product designing plans, and privacy protection policies, so that to attract more consumers. Additionally, social planners also can seek guidelines to

[2] http://www.pwc.com/us/en/press-releases/2014/wearable-technology-future.jhtml.

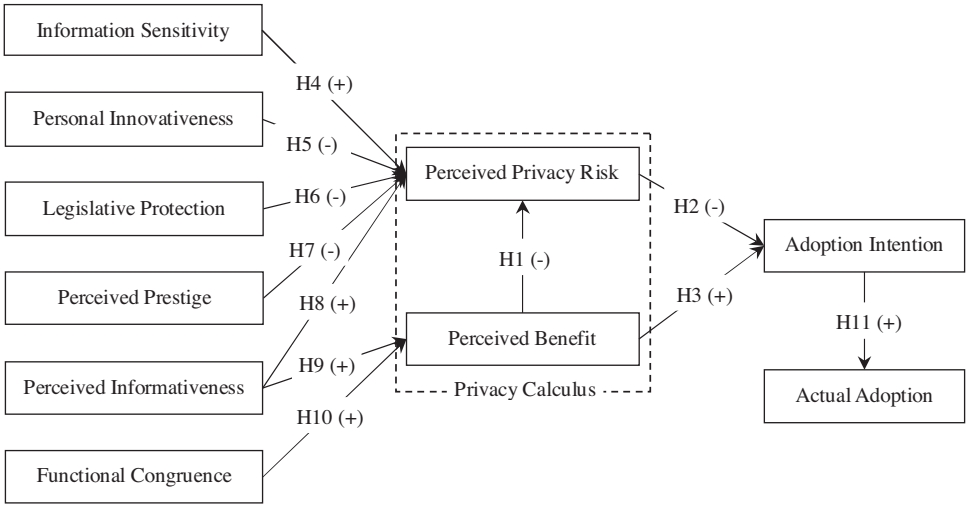

Fig. 1. The research model.

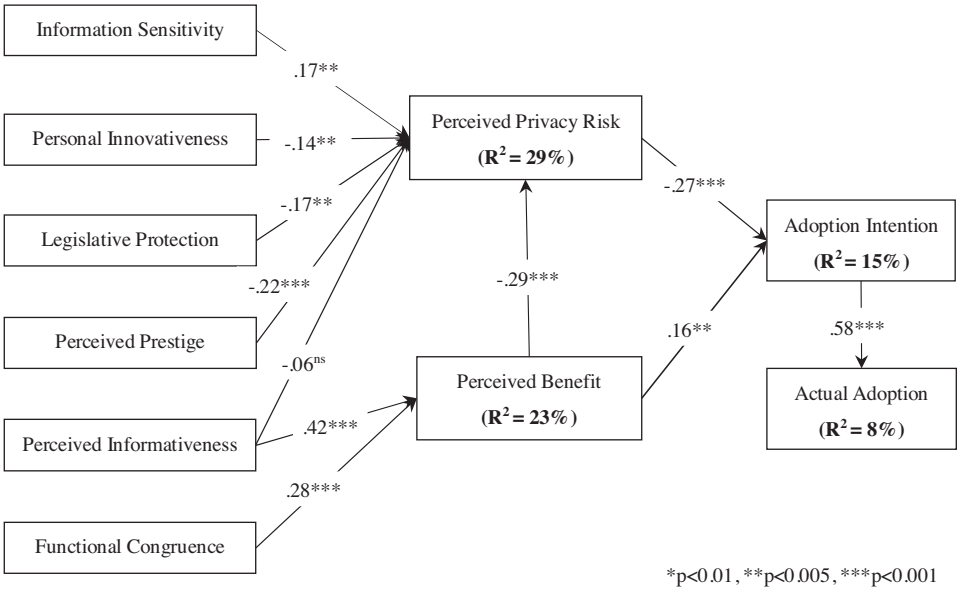

Fig. 2. The structural model.

make better policies to promote the adoption of wearable devices in healthcare sector so that to deliver more effective healthcare services.

The rest of this paper is organized as follows. Section 2 reviews related literature about privacy calculus theory and HIT adoption. The research model and hypotheses are presented in Section 3, which is followed by the research methodology in Section 4. Section 5 deals with the data analysis and results. Conclusion, theoretical and practical implications, and limitations and future research are shown in Section 6.

2. Literature review

This study extends privacy calculus theory to investigate individuals' adoption of healthcare wearable devices. Privacy calculus is originally developed by Laufer and Wolfe [18]. They hold the view that, before disclosing sensitive information, individuals often compare social benefits with latent negative consequences that disclosure will bring. Then the model was applied in Information Systems (IS) field by Culnan and Armstrong [19]. Up to now, privacy calculus theory has been widely adopted to explain consumers' intention to disclose personal information in various contexts, including electronic commerce [20], location-based service [17,21,22], and social commerce [23], etc. However, in e-health context, only a few extant studies have employed privacy calculus theory to examine individuals' health information sharing behaviors [24] as well as their adoption of personal health records (PHR) [15]. Given that wearable devices not only exhibit distinctive advantage on improving healthcare efficiency, but also generate higher level of privacy risk, individuals' decisions to adopt healthcare wearable devices would involve a highly salient privacy calculus in which users may face the tradeoff between perceived benefit and perceived privacy risk [17]. Therefore, privacy calculus theory is more suitable to understand individuals' adoption of healthcare wearable devices.

This research also relates to prior literature about HIT adoption. Extant studies in this field have examined the adoption of various kinds of HIT by individuals and professionals, such as electronic health record (EHR) [25–27], personal health record (PHR) [15,24,26], mobile health service (MHS) [10,12,28,29], clini-

Table 2
The measurement items.

Construct	Items	Reference
Health information sensitivity	HIS1: I do not feel comfortable with the type of health information these wearable devices request from me HIS2: I feel these wearable devices gather highly personal health information about me HIS3: the health information I should provide to these wearable devices is very sensitive to me	[42]
Personal innovativeness in IT	PIIT1: if I heard about a new information technology, I would look for ways to experiment with it PIIT2: among my peers, I am usually the first to try out new information technologies PIIT3: in general, I like to experiment with new information technologies	[70]
Legislative protection	LP1: I believe that I would be protected from the misuse of my personal health data LP2: I believe that the practices of how wearable device providers collect, use, and protect my private health information should be governed and interpreted LP3: I believe that the violation of the health information I provided to wearable devices should be able to be addressed	[42]
Perceived prestige	PP1: people in my community think highly of wearable devices in healthcare PP2: the application of healthcare wearable devices has a good reputation in my community PP3: it is considered positive in the community to adopt healthcare wearable devices	[71]
Perceived informativeness	PIF1: wearable devices are good sources of personal health information PIF2: wearable devices supply relevant health information PIF3: wearable devices are informative about my personal health information	[58]
Functional congruence	FC1: wearable devices are expected to be comfortable FC2: wearable devices are expected to be durable FC3: wearable devices are expected to be priced appropriately considering their quality	[63]
Perceived privacy risk	PPR1: it would be risky to disclose my personal health information to wearable devices vendors PPR2: there would be high potential for loss associated with disclosing my personal health information to vendors providing wearable devices PPR3: there would be too much uncertainty associated with giving my personal health information to vendors providing wearable devices	[15]
Perceived benefit	PB1: using a wearable device would improve my access to my health information PB2: using a wearable device would improve my ability to manage my health PB3: using a wearable device would improve the quality of my healthcare	[15]
Adoption intention	The extent to which I would use wearable devices to seek healthcare is: AI1: unlikely/likely AI2: not probable/probable AI3: unwilling/willing	[72]
Actual adoption behavior	AB1: I have used healthcare wearable device AB2: I use healthcare wearable device to stay on the path of healthy living AB3: I often use healthcare wearable device to get health information	[73]

cal decision support systems (DSS) [30], and biometrics [9]. Various theories have been applied to investigate HIT adoption in these prior studies, including the technology acceptance model (TAM) [9–12,28–32], theory of planned behavior (TPB) [12,29,33,34], and unified theory of use and acceptance of technology (UTAUT) [9,12] from technological perspective; the protection motivation theory (PMT) [12] from healthcare perspective; and privacy calculus theory (PCT) [9,15], social contract theory (SCT) [15], and privacy boundary theory (PBT) [24] from privacy perspective. In addition, some other theories such as elaboration likelihood model (ELM) [25], diffusion of innovation (DOI) [9], identity theory (IDT) [27], and dual factor model (DFM) [32], are also employed to investigate HIT adoption issues. A detailed summary of prior studies about HIT adoption is provided in Table 1.

Different from these related studies, we focus on the empirical examination of individuals' adoption of an understudied and emerging HIT—healthcare wearable device, by considering the distinctive advantages of wearable technology on reducing healthcare cost and improving healthcare efficiency in healthcare sector [35,36]. From Table 1, we can see that most studies about HIT adoption employed technology acceptance theories and healthcare behavior theories to explain user's behaviors toward specific HIT [10–12,24,28,31]. Only a few of them (e.g., Refs. [9,15,37]) have mentioned the privacy issue, but without any further investigation of the formation (antecedents) of individuals' privacy concerns. However, information privacy concern is proved to be more important in the context of HIT than other sectors due to the higher sensitivity of health information [9,15,38]. Therefore, we are going to explore factors that could determine individuals' adoption of healthcare wearable devices, by affecting his/her risk-benefit tradeoff (i.e., privacy calculus). Furthermore, this study also contributes to prior research about healthcare wearable devices that focus on the design of specific wearable devices to be applied in healthcare sector [5–8] and the development of healthcare wearable devices for unique purpose [3,4].

3. Research model and hypothesis

We regard individuals' adoption of healthcare wearable device as dependent variable in our conceptual model (Fig. 1). In line with prior related studies [9,15–17]. we hypothesize that users' decisions to adopt healthcare wearable devices are determined by their tradeoffs between perceived privacy risk and perceived benefit (privacy calculus). In addition, we predict the antecedent effects of health information sensitivity, personal innovativeness, legislative protection, perceived prestige, and perceived informativeness on users' perceived privacy risk. Additionally, we hypothesize that users' perceived benefit is influenced by both, perceived informativeness and functional congruence.

3.1. Privacy calculus

The situation that individuals perform a risk–benefit analysis that accounts for drivers and inhibitors of information disclo-

Table 3
The sample demographics.

Demographic factors		Frequency	Percentage
Gender	Female	172	51.65%
	Male	161	48.35%
Age	25 or under	116	34.83%
	26–35	90	27.03%
	36–45	83	24.92%
	46 or older	44	13.22%
Education	Bachelor	154	46.25%
	Master	145	43.54%
	Doctoral	34	10.21%
Internet experience	Less than 1 year	14	4.20%
	1–2 year	56	16.82%
	3–5 year	124	37.24%
	More than 5 year	139	41.74%
Health status	Healthy	185	55.56%
	Poor health	102	30.63%
	Unhealthy	46	13.81%

sure when they are requested to provide personal information to organizations is generally regarded as privacy calculus [39]. Consistent empirical support for privacy calculus has been achieved in prior studies [17,40]. However, specific antecedents and consequences of privacy calculus may vary depending on different contexts. HIT may aggravate individuals' privacy concerns over the potential misuse of personal health information [15]. Therefore, individuals' decisions to adopt healthcare wearable devices would involve a highly salient privacy calculus in which users may face the tradeoff between perceived benefit and perceived privacy risk [17,41]. When users' perception of benefit exceeds the privacy risk loss, he/she would choose to adopt healthcare wearable devices. Otherwise, the devices would not be adopted [15,21]. Therefore, consistent with prior privacy calculus literature, we make hypotheses given as

H1. Individuals' perceived benefit negatively affects their perceived privacy risk in healthcare wearable device context.

H2. Individuals' perceived privacy risk negatively affects their adoption intention in healthcare wearable device context.

H3. Individuals' perceived benefit positively affects their adoption intention in healthcare wearable device context.

It is critical to note that adoption decisions involve more than a privacy calculus as discussed above [42]. Information disclosure and product purchase entail considerable uncertainties, which also lead to opportunistic behaviors of healthcare wearable devices providers [40]. Thus, we further investigate the antecedents of perceived privacy risk and perceived benefit. We investigate the antecedent effects of health information sensitivity, personal innovativeness in IT, legislative protection, perceived prestige, and perceived informativeness on individuals' perceived privacy risk. In addition, we also predict the antecedent impacts of perceived informativeness and functional congruence on individuals' perceived benefit for healthcare wearable devices. The detail explanations of these relationships are shown in following spaces.

3.2. Antecedents of privacy calculus

Since the use of healthcare wearable device involves both, individuals' healthcare and technology behaviors, we first consider the antecedent effects of health information sensitivity and personal innovativeness on privacy calculus. It has been widely recognized that the type of information collected and used by an organization affects the level of individuals' perceived privacy concerns [42–44]. This information attribute is regarded as 'information sensitivity' in prior privacy studies [44]. On the basis of Malhotra et al. [44] and Dinev et al. [42], we introduce the concept of health information sensitivity as an individual's information attribute that informs the degree of perceived discomfort when disclosing health information to an external agent (a healthcare wearable device provider in our case). When other things being equal, individuals will have more perceptions for privacy risk when disclosing more sensitive information [20,42], because certain domains of life are regarded more private than others [45]. Among prior literature, Dinev et al. [42] have hypothesized and empirically proved the positive impact of information sensitivity on individuals' perceived privacy risk in web 2.0 context. In this paper, considering the widely recognized fact that users are more sensitive on some certain kinds of information such as medical information, personal identifiers, and financial data than other information including demographic information, purchase behaviors, and lifestyle habits [13,14], we hypothesize that

H4. Individuals' perceived health information sensitivity positively affects their perceived privacy risk in healthcare wearable device context.

Except for the healthcare perspective, individuals' adoption of healthcare also shows the information technology (IT) adoption features. We thus also examine the effect of individuals' attitude toward emerging technology (i.e., personal innovativeness in IT) on their risk–benefit tradeoffs in healthcare wearable devices adoption. Personal innovativeness in IT refers to an individual's willingness to try out a new kind of IT [46]. Researchers have made common sense that individuals would react differently due to their differences in characteristics associated with IT innovativeness. Generally, the innovative users are more likely to adopt a new IT even if there is a high level of uncertainty of the adoption [47]. Since a person's attention to privacy would be decreased if he/she has higher innovativeness toward the new IT, an individual's personal innovativeness in IT would decrease his/her perceived privacy risk. Therefore, we hypothesize that

H5. Individuals' personal innovativeness in IT negatively affects their perceived privacy risk in healthcare wearable device context.

Currently, organizations are implementing different strategies, such as building prestige, conducting privacy policies, and third-party assurance, to attract more consumers and reduce their privacy concerns, since they are aware that consumers are more likely to strike back on improper treatment of their personal information [48–50]. Thus, we also investigate the effects of legislative protection and perceived prestige on individuals' privacy calculus in healthcare wearable device context. Prior privacy assurance studies have demonstrated the importance of industry self-regulation and government regulation in users' perceived privacy control and privacy calculus. For instance, Xu et al. [50] have empirically proved the positive effects of proxy control agency (that includes industry self-regulation and government legislation) on individuals' perceived control over personal information. In addition, Dinev et al. [42] proved that regulatory expectations could effectively decrease individuals' perceived privacy risk. Furthermore, Xu et al. [51,17] have indicated the negative effects of both industrial and governmental privacy regulations on privacy risks in various context, such as healthcare, financial, e-commerce, and location-based service. In this paper, we summarize these two regulatory factors as legislative protection, which denotes the privacy regulations that an organization has received, including its own privacy policy and government regulations. In line with prior literatures [17,42,50,51]. we hypothesize that

H6. Individuals' perceived legislative protection negatively affects their perceived privacy risk in healthcare wearable device context.

Table 4
Loadings* and cross-loadings of measures.

Construct	Items	Factor loadings	CR	AVE	Cronbach's α
Health information sensitivity	HIS1	0.872	0.888	0.726	0.864
	HIS2	0.880			
	HIS3	0.802			
Personal innovativeness	PIIT1	0.870	0.889	0.728	0.863
	PIIT2	0.841			
	PIT3	0.848			
Legislative protection	LP1	0.812	0.876	0.703	0.851
	LP2	0.854			
	LP3	0.881			
Perceived prestige	PP1	0.847	0.886	0.722	0.853
	PP2	0.835			
	PP3	0.866			
Perceived informativeness	PIF1	0.848	0.883	0.716	0.855
	PIF2	0.835			
	PIF3	0.856			
Functional congruence	FC1	0.877	0.894	0.738	0.866
	FC2	0.858			
	FC3	0.842			
Perceived privacy risk	PPR1	0.747	0.837	0.633	0.846
	PPR2	0.784			
	PPR3	0.852			
Perceived benefit	PB1	0.849	0.866	0.684	0.860
	PB2	0.802			
	PB3	0.829			
Adoption intention	AI1	0.855	0.882	0.713	0.841
	AI2	0.820			
	AI3	0.858			
Adoption behavior	AB1	0.872	0.882	0.714	0.851
	AB2	0.848			
	AB3	0.814			

* All loadings were statistically significant at level $p < 0.01$.

In addition, we also examine the effect of provider prestige on individuals' privacy calculus. A firm's prestige is an overall assessment of its product and service quality, customer experience, credible communication, and social character of its abilities to satisfy consumers [52]. It provides critical cues of how the firm handles customer affairs, including privacy issues such as the way to collect and use personal information [15]. Extant privacy studies have shown that prestige has direct influence on individuals' information privacy concerns and moderating effect on trust on organizations [49,53,54]. In addition, a firm with higher prestige would enjoy the 'halo effect' [55] since consumers are more likely to believe that the firm can also do better on privacy protection if it is doing excellent jobs in other aspects. However, the disreputable firms may lack the competence to protect privacy. Individuals thus have fewer perceptions on privacy risks when purchasing from a healthcare wearable device provider with higher prestige. Therefore, we hypothesize that

H7. Individuals' perceived prestige negatively affects their perceived privacy risk in healthcare wearable device context.

Since healthcare wearable devices deliver real-time health information through a sensor worn on the body, the product of healthcare wearable device can be considered as both, the delivered health information and the hardware of sensor. We thus investigate the effects of perceived informativeness (information aspect) and functional congruence (hardware perspective) on privacy calculus. Different from the definition of informativeness in marketing [56,57] and website interface designing [58,59] fields, we introduce a new concept of informativeness in healthcare wearable device context as the richness or proportion of healthcare information provided by wearable devices. Theoretically, the informativeness of a healthcare wearable device is also a dimension of the product quality, since it represents the information quality dimension [60]. In addition, if the healthcare wearable devices provide too much personal health information for users, they are more likely to feel uncomfortable about their privacy protection [61,62], which finally may lead to a higher level of perceived privacy risk. Therefore, we propose two hypotheses about the effects of perceived informativeness on privacy calculus in healthcare wearable device context given as

H8. Perceived informativeness positively affects individuals' perceived privacy risk in healthcare wearable device context.

H9. Perceived informativeness positively affects individuals' perceived benefit in healthcare wearable device context.

Functional congruence, a factor adapted from self-congruency theory, refers to the perceived suitability of a product or a brand to fulfill the functional and basic product-related need [63]. Different from other kinds of HIT such as MHS, telemedicine, and clinic DSS, there exists a sensor and its incorporated software in a healthcare wearable device [64]. To monitor personal physical conditions in real-time, the sensor should be worn on the body 24 h a day. This particular characteristic of healthcare wearable device leads to the fact that the material, battery, and comfort are more important than other HITs [2]. Thus, an overall quality that involves the product comfort, function, and battery duration, etc., plays an important role in individuals' assessment of perceived benefit for healthcare wearable devices. We can use functional congruence to represent the overall quality of the device. Therefore, we hypothesize that

H10. Functional congruence positively affects individuals' perceived benefit in healthcare wearable device context.

3.3. Adoption intention and actual behavior

Adoption intention refers to individuals' perceived probability to adopt healthcare wearable devices. Although adoption intention is generally considered as a proxy of behavior in most prior behavioral literature [15,65,66], recent related research has proved that behavioral intention is not a reliable predictor of actual behavior in some certain cases [67–69]. However, in healthcare wearable device context, individuals are more sensitive about their healthcare conditions [42,44] and they are also more eager to adopt emerging technologies to improve their health conditions [25]. Therefore, we hypothesize that

H11. Individuals' intention to adopt healthcare wearable devices positively affects their actual adoption behaviors.

4. Research methodology

4.1. Item development

A survey that included items for the constructs specified in the conceptual model was conducted to collect data that can be used to empirically test the research hypotheses. In order to ensure the content validity, the items for the constructs were developed based on a comprehensive survey of prior privacy literature. The validated standard items were adapted for use as much as possible. All measurement items as shown in Table 2 were adapted from extant research with minor modifications in wording to make them more relevant in healthcare wearable device context. We measure the constructs with 5-point Likert scale items with anchors ranging from 1 'strongly disagree' to 5 'strongly agree'. Since the original questionnaire is in English, we first translated it into Chinese. Three experts in management information systems (MIS) field were invited to examine the question clarity, logical consistency, terminology, translation accuracy, and contextual relevance of the questionnaire in both, English and Chinese versions. Comments and suggestions collected from these experts lead to some minor modifications through further discussion. In addition, we conducted a pilot study involving 24 undergraduate students at MIS department. The respondents' feedback and analysis of the measurement model lead to some minor modifications, including the wording of items, deleting certain items, and editing the instructions.

4.2. Study design and procedure

The survey was administrated in two large social network groups that relate to healthcare wearable devices, since most members in the groups are more interested in and familiar with healthcare wearable devices. At the beginning of the survey, the candidates were required to read an informed consent form. If they agreed to take the survey, a question of whether they have used wearable devices in the past was required to answer, so that to guarantee the respondents are actual users of healthcare wearable devices. There were 374 participants involved in the survey. By removing the unusable responses that include missing answers for any item, a total of 333 responses were used in data analysis. The ANOVA analysis was utilized to compare the demographics of the participants from these two groups. No significant differences were found. We also have checked their ages, genders, education levels, experiences, and health statuses in the groups. In general, we conclude that our sample exhibits satisfactory representation to study wearable technology adoption in healthcare. The detailed respondent demographics are provided in Table 3.

Table 5
Discriminant validity: the square root of AVEs and factor correlation coefficients.

Constructs	HIS	PIIT	LP	PP	PIF	FC	PPR	PB	AI	AB
HIS	**.852**									
PIIT	−.211	**.853**								
LP	−.220	.250	**.838**							
PP	−.267	.279	.134	**.849**						
PIF	−.174	.283	.240	.215	**.846**					
FC	−.284	.278	.199	.199	.031	**.859**				
PPR	.333	−.334	−.320	−.367	−.269	−.139	**.796**			
PB	−.255	.196	.317	.233	.338	.251	−.423	**.827**		
AI	−.179	.254	.185	.170	.235	.176	−.306	.268	**.845**	
AB	−.221	.211	.145	.209	.253	.252	−.251	.315	.220	**.845**

Note: the square root of AVE is denoted in bold.

Table 6
The summary of model fit indices.

Index	Observed value	Recommended value	References
χ^2/d.f.	1.998	Less than 3	[77]
GFI	0.852	Greater than 0.80	[78]
AGFI	0.826	Greater than 0.80	[78]
NFI	0.862	Greater than 0.80	[77]
IFI	0.926	Greater than 0.90	[78]
CFI	0.925	Greater than 0.90	[77]
RMSEA	0.055	Less than 0.08	[78]

5. Data analysis and results

In this study, SEM is employed to test hypotheses. We analyzed our data following Anderson and Gerbing's [74] two-step approach: measurement model and structural model.

5.1. Measurement model

To evaluate measurement model, confirmatory factor analysis (CFA) was adopted to test whether the constructs have sufficient reliability and validity [42,75,76]. First, we examined the reliability of the construct using Cronbach's α, composite reliability (CR) and average variance extracted (AVE). Cronbach's α scores for constructs range from 0.841 to 0.866, which surpass the recommended value of 0.7. As shown in Table 4, the CR value of each construct is higher than the threshold 0.6, and AVE of all constructs exceed the recommended value 0.5. Thus, Cronbach's α, CR, and AVE values indicate sufficient reliability of measurement model.

In addition, validity is measured by content validity and construct validity. The variables in this study are all derived from existing research, thus exhibiting good content validity. Convergent validity and discriminant validity are employed to evaluate construct validity. The convergent validity can be assessed by item loading coefficient and average variance extracted (AVE). The item loading coefficient surpasses the lowest score 0.6 and its cross-loading coefficient is below 0.4 at the significant level of $p < 0.001$, supporting the convergent validity of measurement scales. The discriminant validity is assessed by the use of the square root of AVE. The square root of AVE is greater than the correlations between the construct and the other constructs, which confirms the discriminant validity of the constructs. The details of discriminant validity test are shown in Table 5.

5.2. Structural model

After assessing the validity and reliability of the measurement model, we tested the structural model. To examine the degree to which the model represents the data, we use AMOS 17.0 to evaluate the "Goodness of Fit" indices. The results as shown in Table 6 indicate that all indices are within the commonly accepted thresh-

olds. The results demonstrate that the model exhibits a reasonably good fit to the empirical data.

5.3. Hypotheses testing results

The results of hypotheses testing are shown in Fig. 2. The results show that perceived benefit has significant negative effect on individuals' perceived privacy risk, indicating that individuals' perceived benefit for healthcare wearable devices would decrease their privacy risk perception. In addition, perceived benefit has been proved to positively affect individuals' intention to adopt healthcare wearable devices, and perceived privacy risk negatively affects individuals' intention to adopt healthcare wearable device. By comparing the coefficient and significance level of these three relationships in privacy calculus framework, we can observe that perceived privacy risk plays a more important role in individuals' intention to adopt healthcare wearable devices, because the absolute value of the coefficient is higher than the others, and it also exhibits highest significant level. This unique finding also demonstrates that privacy issue is quite important in healthcare wearable devices context.

Another group of main findings in this paper is related to the antecedents of perceived privacy risk in healthcare wearable devices context. First, both, health information sensitivity and personal innovativeness have significant effects on individuals' perceived privacy risk, and these two relationships are significant at level of 99.5%. Second, legislative protection and perceived prestige negatively affects individuals' perceived privacy risk of healthcare wearable devices adoption at level of 99.5% and 99.9%, respectively. These results are consistent with the results of prior studies such as Dinev et al. [42] and Li [79]. Specially, we find that healthcare wearable devices providers' prestige has more influence on individuals' privacy risk perception with higher coefficient at a larger significant level, which is quite different from prior privacy literature [15,50,80].

However, the hypothesized positive effect of perceived informativeness on individuals' perceived privacy risk was not statistically supported. In addition, the data analysis results show that the impact of perceived informatives on perceived privacy risk was also not positive, which is contrary to the hypothesis. The main reason is that perceived informativeness has more influence on perceived benefit than perceived privacy risk, and perceived benefit would decrease the perception of privacy risk. Thus, the effect of perceived informativeness on perceived privacy risk would be negative and not significant.

Furthermore, we also have obtained the findings about the antecedents of individuals' perceived benefit of adopting healthcare wearable devices. Both, perceived informativeness and functional congruence significantly affect individuals' perceived benefit for healthcare wearable devices at significance level of 99.9%. Put all findings together, we can see that perceived prestige, functional congruence, and perceived privacy risk have more important effects on individuals' decisions to adopt healthcare wearable devices than other factors, since their absolute value of coefficient and significant level are higher than others. These three critical factors are still understudied in extant literature on HIT adoption [10–12,24,28,31] and information privacy concerns [42,51,65]. They also exhibit unique characteristics in healthcare wearable devices context.

Finally, although some recent studies have demonstrated that the intention is not a good predictor of actual behavior [67–69]. our study is proved to be consistent with prior research argues that behavioral intention is a good proxy of actual behavior. The most possible reason is that most of these studies focus on educational context, which represent a passive intention. However, healthcare wearable devices are personal electronics, thus the intention to use is more intensive, which causes actual behavior more easily.

6. Conclusion and discussions

This study attempted to provide an early empirical support for a model that examines the predictors of individuals' adoption of healthcare wearable devices from privacy calculus perspective. Drawing on the privacy calculus theory, we developed a model suggesting that in addition to the impacts of perceived privacy risk and perceived benefit on individuals' adoption of healthcare wearable devices, individuals' perceived privacy risk is determined by health information sensitivity, personal innovativeness, legislative protection, and perceived prestige. Individuals' perceived benefit is affected by perceived informativeness and functional congruence. The proposed conceptual model was empirically tested through a survey.

As shown in the path analysis results (Fig. 2), 10 hypotheses were statistically significant. From the results, we can see that the privacy calculus indeed exists in individuals' adoption of healthcare wearable devices. In other words, the negative effect of perceived benefit on individuals' perceived privacy risk, the positive impact of perceived benefit on individuals' adoption intention, and the negative influence of perceived privacy risk on individuals' adoption intention are all statistically significant in the context of healthcare wearable devices. Thus, H1–H3 in the model are supported, respectively. In addition, health information sensitivity, personal innovativeness, legislative protection, and perceived prestige are proved to significantly affect individuals' perceived privacy risk for healthcare wearable devices, thus supporting H4–H7, respectively. Additionally, perceived benefit for healthcare wearable devices is significantly affected by perceived informativeness and functional congruence, which support H9 and H10, respectively. Furthermore, the influence of perceived informativeness on perceived privacy risk is not statistically significant, which indicates that H8 is not supported in healthcare wearable device context. Also the adoption intention is significant positively related to the actual adoption behavior, so the H11 is also verified in this study.

6.1. Theoretical and practical implications

This study makes several theoretical contributions to prior related literature. First, we are among the first to investigate healthcare wearable devices issue from behavioral perspective. Different from prior related studies on developing healthcare wearable technology and specific wearable devices to be applied in healthcare field, this study has potentials to provide theoretical foundations for the understanding of individuals' behaviors toward healthcare wearable devices. In addition, different from prior literature on individuals' adoption of different HITs such as MHS, telemedicine, and clinical DSS from technology and healthcare perspective, this study explored the predictors of consumers' decisions to adopt a new kind of HIT—healthcare wearable devices, from privacy calculus perspective. This research enhanced our understanding of individuals' privacy perceptions and calculus in their decisions to adopt emerging HIT. Furthermore, different from extant literature on empirically examining individuals' adoption of HIT based on technology acceptance models such as TAM, TPB, and UTAUT, this research has proved the effectiveness of privacy calculus theory on understanding users' adoption of HIT. Future studies about HIT adoption should not only focus on technology acceptance perspective, but also should consider individuals' privacy calculus. Other domains that exhibit higher privacy risk also should pay more attention to the privacy issue when understanding individuals' adoption behaviors.

Summary points
What was already known on the topic?

- Healthcare wearable technology has distinctive advantages on improving healthcare efficiency and reducing healthcare cost.
- Individual's privacy perception plays an important role in the adoption of health information technology that includes healthcare wearable devices.

What this study has added to the body of knowledge?

- Based on privacy calculus theory, we develop and validate a more comprehensive model to understand individual's decision to adopt healthcare wearable devices.
- This study sheds new light on understanding the formation of individual's privacy calculus in the context of healthcare wearable devices.
- This research provides insights for business managers and social planners to conduct better strategies and policies to promote wearable devices adoption in healthcare sector.

In addition, this study also exhibits several practical implications for business managers and social planners. On one side, healthcare wearable devices managers can seek guidelines on how to make better strategies to attract more consumers. For instance, according to our results, managers can build better prestige for their brands and products through improving product and service quality, making better privacy policies to protect individuals' health information privacy, making efforts on the product comfort and battery duration, providing higher quality health information that can satisfy consumers' demands, and supplying satisfactory plans when privacy intrusion occurs, etc. On the other side, social planners also can be guided to promote healthcare wearable devices adoption. For example, they can make more regulations on the way that healthcare wearable devices firms collect and use individuals' personal health data. In addition, they also can make efforts on helping individuals to know more about healthcare wearable devices and providing enough incentives for them to adopt the devices. Furthermore, another strategy that social planners can adopt is to increase the entry standards in terms of product quality and privacy policy so that the overall product quality and organization prestige can be increased.

6.2. Limitations and future research

Although this research provides several theoretical and practical contributions and most hypotheses were supported by the empirical data, this study still has some potential limitations. First of all, our model explains 15% of the adoption intention variance, and 8% of the actual adoption variance, which are not particularly high predictive powers. The main reason is that we did not include many other factors that could also affect individuals' adoption of healthcare wearable devices, such as TAM and UTAUT predictors. Therefore, future studies should control these potential predictors of healthcare wearable devices adoption. In addition, the survey data was collected at a single point in time. However, measurement of new IT adoption is more likely to involve retrospective analysis. Hence, future studies can make a longitudinal investigation to obtain more convincing explanation on how individuals' adoption behaviors toward healthcare wearable devices changes over time. Furthermore, our empirical study is restricted to a Chinese sample, which has not considered the cultural and technological differences among different countries. It would be necessary to test whether the results hold in other countries such as the U.S., European countries, and other Asian countries. Therefore, an alternative way to extend this study would be to conduct a comparative study of healthcare wearable devices adoption between different countries.

Conflict of interest

No conflict of interest exists in this paper.

Authors' contributions

Each co-author of this paper has been involved in research design, data collection, data analysis, and the paper writing and proving.

References

[1] C. Wolff, Wearable in the workplace, Harv. Bus. Rev. 91 (2013) 23–25.
[2] M. Chan, D. Estève, J.-Y. Fourniols, C. Escriba, E. Campo, Smart wearable systems: current status and future challenges, Artif. Intell. Med. 56 (2012) 137–156.
[3] S. Harris, Catwalk goes techno (wearable technologies), Eng. Technol. 3 (2008) 28–30.
[4] J. Keller, Rapid pace of commercial technology complicates Army plans for wearable computing, Mil. Aerosp. Electron. 24 (2013) 28–29.
[5] Y.-L. Zheng, X.-R. Ding, C.C.Y. Poon, B.P.L. Lo, H. Zhang, X.-L. Zhou, G.-Z. Yang, N. Zhao, Y.-T. Zhang, Unobtrusive sensing and wearable devices for health informatics, IEEE Trans. Biomed. Eng. 61 (2014) 1538–1554.
[6] S. Moran, T. Nishida, K. Nakata, Comparing British and Japanese perceptions of a wearable ubiquitous monitoring device, IEEE Technol. Soc. Mag. 32 (2013) 45–49.
[7] M. Markovic, M. Rapin, M. Correvon, Y. Perriard, Design and optimization of a blood pump for a wearable artificial kidney device, IEEE Trans. Ind. Appl. 49 (2013) 2053–2060.
[8] G.K.J. Lewis, M.D. Langer, C.R.J. Henderson, R. Ortiz, Design and evaluation of a wearable self-applied therapeutic ultrasound device for chronic myofascial pain, Ultrasound Med. Biol. 39 (2013) 1429–1439.
[9] C.L. Miltgen, A. Popovič, T. Oliveira, Determinants of end-user acceptance of biometrics: Integrating the Big 3 of technology acceptance with privacy context, Decis. Support Syst. 56 (2013) 103–114.
[10] X. Lishan, Y.C. Chiuan, M. Choolani, C.H. Chuan, The perception and intention to adopt female-focused healthcare applications (FHA): a comparison between healthcare workers and non-healthcare workers, Int. J. Med. Inform. 78 (2009) 248–258.
[11] T.T. Moores, Towards an integrated model of IT acceptance in healthcare, Decis. Support Syst. 53 (2012) 507–516.
[12] Y. Sun, N. Wang, X. Guo, Z. Peng, Understanding the acceptance of mobile health services: a comparison and integration of alternative models, J. Electron. Comm. Res. 14 (2013) 183–200.
[13] N. Vidmar, D.H. Flaherty, Concern for personal privacy in an electronic age, J. Commun. 35 (1985) 91–103.
[14] T. Dinev, P. Hart, Privacy concerns and levels of information exchange: An empirical investigation of intended e-services use, E-serv. J. 4 (2006) 25–59.
[15] Y. Li, The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns, Decis. Support Syst. 57 (2014) 343–354.
[16] T. Dinev, M. Bellotto, P. Hart, V. Russo, I. Serra, C. Colautti, Privacy calculus model in e-commerce—a study of Italy and the United States, Eur. J. Inform. Syst. 15 (2006) 389–402.
[17] H. Xu, H.-H. Teo, B.C.Y. Tan, R. Agarwal, The role of push–pull technology in privacy calculus: the case of location-based services, J. Manage. Inform. Syst. 26 (2009) 135–173.
[18] R.S. Laufer, M. Wolfe, Privacy as a concept and a social issue: a multidimensional developmental theory, J. Social Issues 33 (1977) 22–42.
[19] M.J. Culnan, P.K. Armstrong, Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation, Org. Sci. 10 (1999) 104–115.
[20] H. Li, R. Sarathy, H. Xu, The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors, Decis. Support Syst. 51 (2011) 434–445.
[21] H. Xu, X. Luo, J.M. Carroll, M.B. Rosson, The personalization privacy paradox: an exploratory study of decision making process for location-aware marketing, Decis. Support Syst. 51 (2011) 42–52.
[22] L. Zhao, Y. Lu, S. Gupta, Disclosure intention of location-related information in location-based social network services, Int. J. Electron. Comm. 16 (2012) 53–90.
[23] S. Sharma, R.E. Crossler, Disclosing too much? Situational factors affecting information disclosure in social commerce environment, Electron. Comm. Res. Appl. 13 (2014) 305–319.

[24] C.L. Anderson, R. Agarwal, The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information, Inform. Syst. Res. 22 (2011) 469–490.
[25] C.M. Angst, R. Agarwal, Adoption of electronic health records in the presence of privacy concerns: the elaboration likelihood model and individual persuasion, MIS Q. 33 (2009) 339–370.
[26] Z. Ozdemir, J. Barron, S. Bandyopadhyay, An analysis of the adoption of digital health records under switching costs, Inform. Syst. Res. 22 (2011) 491–503.
[27] A.N. Mishra, C. Anderson, C.M. Angst, R. Agarwal, Electronic health records assimilation and physician identity evolution: an identity theory perspective, Inform. Syst. Res. 23 (2012) 738–760.
[28] S. Lim, L. Xue, C.C. Yen, L. Chang, H.C. Chan, B.C. Tai, H.B.L. Duh, M. Choolani, A study on Singaporean women's acceptance of using mobile phones to seek health information, Int. J. Med. Inform. 80 (2011) e189–e202.
[29] I.-L. Wu, J.-Y. Li, C.-Y. Fu, The adoption of mobile healthcare by hospital's professionals: an integrative perspective, Decis. Support Syst. 51 (2011) 587–596.
[30] M.P. Johnson, K. Zheng, R. Padman, Modeling the longitudinality of user acceptance of technology with an evidence-adaptive clinical decision support system, Decis. Support Syst. 57 (2014) 444–453.
[31] W. Maass, U. Varshney, Design and evaluation of ubiquitous information systems and use in healthcare, Decis. Support Syst. 54 (2012) 597–609.
[32] X. Guo, Y. Sun, N. Wang, Z. Peng, Z. Yan, The dark side of elderly acceptance of preventive mobile health services in China, Electron. Markets 23 (2013) 49–61.
[33] S.-Y. Hung, J.C.-A. Tsai, C.-C. Chuang, Investigating primary health care nurses' intention to use information technology: an empirical study in Taiwan, Decis. Support Syst. 57 (2014) 331–342.
[34] Z. Deng, X. Mo, S. Liu, Comparison of the middle-aged and older users' adoption of mobile health services in China, Int. J. Med. Inform. 83 (2014) 210–224.
[35] M.L. Berger, C. Lipset, A. Gutteridge, K. Axelsen, P. Subedi, D. Madigan, Optimizing the leveraging of real-world data to improve the development and use of medicines, Value Health 18 (2015) 127–130.
[36] S. Safavi, Z. Shukur, Conceptual privacy framework for health information on wearable device, PLoS One 9 (2014) 1–16.
[37] Y. Gao, H. Li, Y. Luo, An empirical study of wearable technology acceptance in healthcare, Ind. Manage. Data Syst. 119 (2015) 1704–1723.
[38] M.V. Laric, D.A. Pitta, L.P. Katsanis, Consumer concerns for healthcare information privacy: a comparison of U.S. and Canadian perspectives, Res. Healthc. Financ. Manage. 12 (2009) 93–111.
[39] N.F. Awad, M. Krishnan, The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization, MIS Q. 30 (2006) 13–28.
[40] T. Dinev, P. Hart, An extended privacy calculus model for e-commerce transactions, Inform. Syst. Res. 17 (2006) 61–80.
[41] H. Li, J. Wu, L. Liu, Q. Li, Adoption of big data analytics in healthcare: the efficiency and privacy, in: Proceedings of 19th Pacific Asia Conference on Information Systems, Singapore, 2015 http://aisel.aisnet.org/pacis2015/181.
[42] T. Dinev, H. Xu, J.H. Smith, P. Hart, Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts, Eur. J. Inform. Syst. 22 (2013) 295–316.
[43] G.R. Milne, M.E. Gordon, Direct mail privacy-efficiency trade-offs within an implied social contract framework, J. Public Policy Market. 12 (1993) 206–215.
[44] N.K. Malhotra, S.S. Kim, J. Agarwal, Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model, Inform. Syst. Res. 15 (2004) 336–355.
[45] J. Phelps, G. Nowak, E. Ferrell, Privacy concerns and consumer willingness to provide personal information, J. Public Policy Market. 19 (2000) 27–41.
[46] R. Agarwal, J. Prasad, A conceptual and operational definition of personal innovativeness in the domain of information technology, Inform. Syst. Res. 9 (1998) 204–215.
[47] O. Kwon, K. Choi, M. Kim, User acceptance of context-aware services: self-efficacy, user innovativeness and perceived sensitivity on contextual pressure, Behav. Inform. Technol. 26 (2007) 483–498.
[48] L.N. Zlatolas, T. Welzer, M. Heričko, M. Hölbl, Privacy antecedents for SNS self-disclosure: the case of Facebook, Comput. Hum. Behav. 45 (2015) 158–167.
[49] D.J. Kim, D.L. Ferrin, H.R. Rao, A trust-based consumer decision-making model in electronic commerce: the role of trust, perceived risk, and their antecedents, Decis. Support Syst. 44 (2008) 544–564.
[50] H. Xu, H.-H. Teo, B.C.Y. Tan, R. Agarwal, Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services, Inform. Syst. Res. 23 (2012) 1342–1363.
[51] H. Xu, D. Tamara, S. Jeff, H. Paul, Information privacy concerns: linking individual perceptions with institutional privacy assurances, J. Assoc. Inform. Syst. 12 (2011) 798–824.
[52] A. Riahi-Belkaoui, E.L. Pavlik, Accounting for Corporate Reputation, Praeger Pub Text, 1992.
[53] M.A. Eastlick, S.L. Lotz, P. Warrington, Understanding online B-to-C relationships: an integrated model of privacy concerns, trust, and commitment, J. Bus. Res. 59 (2006) 877–886.
[54] E.B. Andrade, V. Kaltcheva, B. Weitz, Self-disclosure on the web: the impact of privacy policy, reward, and company reputation, Adv. Consum. Res. 29 (2002) 350–353.
[55] B. Jin, J.Y. Park, J. Kim, Joint influence of online store attributes and offline operations on performance of multichannel retailers, Behav. Inform. Technol. 29 (2010) 85–96.
[56] G. Taylor, The informativeness of on-line advertising, Int. J. Ind. Org. 29 (2011) 668–677.
[57] Y.J. Kim, J. Han, Why smartphone advertising attracts customers: a model of web advertising, flow, and personalization, Comput. Hum. Behav. 33 (2014) 256–269.
[58] A.V. Hausman, J.S. Siekpe, The effect of web interface features on consumer online purchase intentions, J. Bus. Res. 62 (2009) 5–13.
[59] Y.-S. Kang, Y.J. Kim, Do visitors' interest level and perceived quantity of web page content matter in shaping the attitude toward a web site? Decis. Support Syst. 42 (2006) 1187–1202.
[60] P.E. Dimitropoulos, D. Asteriou, The effect of board composition on the informativeness and quality of annual earnings: empirical evidence from Greece, Res. Int. Bus. Finance 24 (2010) 190–205.
[61] S.M. Meystre, Ó. Ferrández, F.J. Friedlin, B.R. South, S. Shen, M.H. Samore, Text de-identification for privacy protection: a study of its impact on clinical text information content, J. Biomed. Inform. 50 (2014) 142–150.
[62] C.E. Tucker, The economics of advertising and privacy, Int. J. Ind. Org. 30 (2012) 326–329.
[63] F. Huber, K. Vollhardt, I. Matthes, J. Vogel, Brand misconduct: consequences on consumer–brand relationships, J. Bus. Res. 63 (2010) 1113–1120.
[64] J. Wei, How wearables intersect with the cloud and the internet of things, IEEE Consum. Electron. Mag. 3 (2014) 53–56.
[65] T. Wang, C.-H. Jung, M.-H. Kang, Y.-S. Chung, Exploring determinants of adoption intentions towards Enterprise 2.0 applications: an empirical study, Behav. Inform. Technol. 33 (2014) 1048–1064.
[66] Y. Li, Theories in online information privacy research: a critical review and an integrated framework, Decis. Support Syst. 54 (2012) 471–481.
[67] N. Nistor, When technology acceptance models won't work: non-significant intention-behavior effects, Comput. Hum. Behav. 34 (2014) 299–300.
[68] C. Harrison, C. Tomás, C. Crook, An e-maturity analysis explains intention—behavior disjunctions in technology adoption in UK schools, Comput. Hum. Behav. 34 (2014) 345–351.
[69] Á.F. Agudo-Peregrina, Á. Hernández-García, F.J. Pascual-Miguel, Behavioral intention, use behavior and the acceptance of electronic learning systems: differences between higher education and lifelong learning, Comput. Hum. Behav. 34 (2014) 301–314.
[70] D.R. Compeau, C.A. Higgins, Computer self-efficacy: development of a measure and initial test, MIS Q. 19 (1995) 189–211.
[71] T.B. Cornwell, L.V. Coote, Corporate sponsorship of a cause: the role of identification in purchase intent, J. Bus. Res. 58 (2005) 268–276.
[72] G. Bansal, F.M. Zahedi, D. Gefen, The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online, Decis. Support Syst. 49 (2010) 138–150.
[73] T. Zhou, Y. Lu, B. Wang, Integrating TTF and UTAUT to explain mobile banking user adoption, Comput. Hum. Behav. 26 (2010) 760–767.
[74] J.C. Anderson, D.W. Gerbing, Structural equation modeling in practice: a review and recommended two-step approach, Psychol. Bull. 103 (1988) 411.
[75] D.T. Campbell, D.W. Fiske, Convergent and discriminant validation by the multitrait-multimethod matrix, Psychol. Bull. 56 (1959) 81–105.
[76] D. Straub, M.-C. Boudreau, D. Gefen, Validation guidelines for IS positivist research, Commun. Assoc. Inform. Syst. 13 (2004) 380–427.
[77] C. Fornell, D.F. Larcker, Evaluating structural equation models with unobservable variables and measurement error, J. Market. Res. 18 (1981) 39–50.
[78] J.F. Hair, R.E. Anderson, R.L. Tatham, W.C. Black, Multivariate Data Analysis, Prentice-Hall, Englewood Cliffs, NJ, 1998.
[79] Y. Li, Empirical studies on online information privacy concerns: literature review and an integrative framework, Commun. Assoc. Inform. Syst. 28 (2011) 453–496.
[80] K.A. Stewart, A.H. Segars, An empirical examination of the concern for information privacy instrument, Inform. Syst. Res. 13 (2002) 36–49.