AIS Transactions on Human-Computer Interaction

Volume 14 | Issue 4 Article 3

12-31-2022

The Role of the Privacy Calculus and the Privacy Paradox in the Acceptance of Wearables for Health and Wellbeing

Thomas Jernejcic
California Baptist University, tjernejcic@calbaptist.edu

Omar El-Gayar
Dakota State University, omar.el-gayar@dsu.edu

Recommended Citation

Jernejcic, T., & El-Gayar, O. (2022). The Role of the Privacy Calculus and the Privacy Paradox in the Acceptance of Wearables for Health and Wellbeing. *AIS Transactions on Human-Computer Interaction, 14*(4), 490-522. https://doi.org/10.17705/1thci.00177
DOI: 10.17705/1thci.00177

Transactions on Human-Computer Interaction

Volume 14 Issue 4

12-2022

The Role of the Privacy Calculus and the Privacy Paradox in the Acceptance of Wearables for Health and Wellbeing

Thomas Jernejcic

Jabs School of Business, California Baptist University, tjernejcic@calbaptist.edu

Omar El-Gayar

College of Business and Information Systems, Dakota State University, omar.el-gayar@dsu.edu

Recommended Citation

Jernejcic, T., & El-Gayar, O. (2022). The role of the privacy calculus and the privacy paradox in the acceptance of wearables for health and wellbeing. *AIS Transactions on Human-Computer Interaction*, *14*(4), pp. 490-522.

DOI: 10.17705/1thci.00177

Available at http://aisel.aisnet.org/thci/vol14/iss4/3

Transactions on Human-Computer Interaction

Research Paper DOI: 10.17705/1thci.00177 ISSN: 1944-3900

The Role of the Privacy Calculus and the Privacy Paradox in the Acceptance of Wearables for Health and Wellbeing

Thomas Jernejcic
Jabs School of Business, California Baptist University

Omar El-Gayar
College of Business and Information Systems, Dakota State University

Abstract:

The Internet along with innovations in technology have inspired an industry focused on designing portable devices, known as wearables that can track users' personal activities and wellbeing. While such technologies have many benefits, they also have risks (especially regarding information privacy and security). These concerns become even more pronounced with healthcare-related wearables. Consequently, users must consider the benefits given the risks *(*privacy calculus*)*; however, users often opt for wearables despite their disclosure concerns *(*privacy paradox*)*. In this study, we investigate the multidimensional role that privacy (and, in particular, the privacy calculus and the privacy paradox) plays in consumers' intention to disclose their personal information, whether health status has a moderating effect on the relationship, and the influence of privacy on acceptance. To do so, we evaluated a research model that explicitly focused on the privacy calculus and the privacy paradox in the healthcare wearables acceptance domain. We used a survey-oriented approach to collect data from 225 users and examined relationships among privacy, health, and acceptance constructs. In that regard, our research confirmed significant evidence of the influence of the privacy calculus on disclosure and acceptance as well as evidence of the privacy paradox when considering health status. We found that consumers felt less inclined to disclose their personal information when the risks to privacy outweighed benefits; however, health status moderated this behavior such that people with worse health tipped the scale towards disclosure. This study expands our previous knowledge about healthcare wearables' privacy/acceptance paradigm and, thus, the influences that affect healthcare wearables' acceptance in the privacy context.

Keywords: Privacy, Wearables, Healthcare, Privacy Calculus, Privacy Paradox, Technology Acceptance

Jia Shen was the accepting senior editor for this paper.

1 Introduction

Wearables refer to portable computing devices that users wear and that have specific and/or specialized functions (Jayden, 2018). More specifically, healthcare-related wearables refer to wearables that support one's health and wellbeing as opposed to wearables that do not provide any health-related functionality (see Figure 1). Healthcare-related wearables typically come in two types: 1) fitness wearable devices and 2) medical wearable devices (Gao et al., 2015). The former supports users' basic fitness via monitoring data such as exercise and sleep, whereas the latter addresses specific health-related conditions and illnesses such as high blood pressure and diabetes. Healthcare-related wearables provide many benefits; for example, they can improve one's health and wellbeing (Jayden, 2018), encourage physical activity (Meyer et al., 2015), allow healthcare practitioners to remotely monitor one's health (Nadeem et al., 2015), and provide chronic-illness support (Nadeem et al., 2015). As a result, healthcare wearables can provide users with a better quality of life, reduce their medical costs, and help them recognize events before they occur (Anaya et al., 2018).

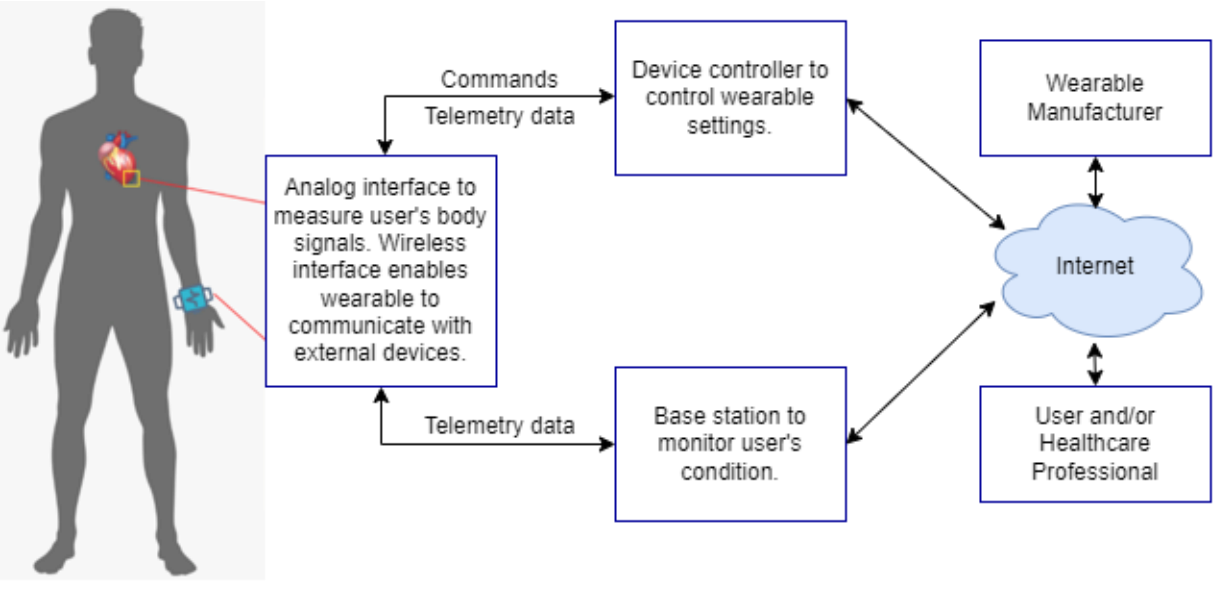

Figure 1. Wearable System Architecture (Adapted from Hassija et al., 2021)

One can classify wearables as consumer wearables or special-purpose wearables (Perez & Zeadally, 2018)) and, further, into several different categories such as smartwatches (Kritzler et al., 2015), body motion trackers (Yang et al., 2016), implantables, performance monitors, heart rate monitors (Muaremi et al., 2013), pedometers (Zenonos et al., 2016), and blood pressure monitors (Nadeem et al., 2015). Wearables accommodate diverse body placements, such as the wrist, chest, stomach, arm, head, thigh, waist, knee, ankle, back, finger, neck, pocket, and over the body (Jayden, 2018). Special-purpose wearables include Internet of things (IoT)-enabled baby clothes designed to monitor a child's temperature, respiration, and activity levels (GAO, 2017). These adaptable characteristics solicit various uses and promise significant appeal for years to come.

While we can attribute definite health benefits to wearables, they also come with substantial risks, especially in the privacy and security realm. Merriam-Webster defines privacy as "freedom from unauthorized intrusion" ("Privacy", 2017). When applied to personal privacy, we can restate this definition as one's control over disclosing their personal information (Bélanger & Crossler, 2011). More specifically, it refers to the authority that one has over their personal information regarding how, when, and to what extent others will distribute it (Romano & Fjermestad, 2007). The concern about privacy rises to the surface considering that wearables frequently lack designs that protect users' information or that do so poorly (Wei & Piramuthu, 2014). The issue becomes even more prominent when one considers that compromised health-oriented devices such as implantable medical devices (IMDs) could threaten people's life or wellbeing (Zhou et al., 2019). For example, in 2007, United States Vice President Dick Cheney reportedly requested his physician to disable Internet access to his pacemaker due to assassination concerns (Hassija et al., 2021).

In the wearable context, data is particularly at risk for two reasons. First, before transmission, wearable devices store data in them; and, as we note above, they often lack sufficient security features (Wei & Piramuthu, 2014). Second, once a wearable has transmitted data, it resides in a vendor and/or cloud environment, which the vendor and/or other third-party entities can access (Padyab & Ståhlbröst, 2018). Considering a wearable device's context and purpose, the information stored will include personal information (Padyab & Ståhlbröst, 2018). At minimum, the information will represent monitored activities; however, it could also include personally identifiable information (PII) and health-related data that the user may not want others to know.

The decision process to adopt wearables involves many facets. Users must weigh benefits against risks, which researchers recognize as the privacy calculus (Smith et al., 2011). While benefits entice individuals to pursue the technology, risks can prevent them from doing so. Many individuals recognize the potential for others to misuse their private information. For example, over 94 percent of Americans have reportedly exhibited such concerns (Malhotra et al., 2004), and 43 percent of consumers have acknowledged discomfort with sharing any personal data (Perez, 2018). Often, although concerned with their privacy, users will openly opt to use a wearable and relinquish concerns with whether it or third parties will disclose their information, which researchers recognize as the privacy paradox (Barth & de Jong, 2017; Norberg et al., 2007; Spiekermann et al., 2001). The privacy paradox combines averseness to disclose with acceptance to disclose.

While past research focused on privacy in the wearable technology domain (e.g., Lehto & Lehto, 2017; Vitak et al., 2018; Meyer et al., 2015; Preusse et al., 2017) have investigated reasons and benefits for accepting the technology, we lack research that has examined the multi-dimensional role that privacy plays in the decision-making process and, in particular, the impact that the privacy calculus has on the intention to disclose private information and the downstream effect regarding (healthcare-related) wearables' acceptance and use. Accordingly, in this study, we explore constructs and relationships related to the privacy calculus to determine how those constructs in aggregate influence (or fail to influence) a person's inclination to adopt a healthcare wearable device. Specifically, we address the following research questions (RQ):

RQ1: To what extent does the privacy calculus impact people's intention to disclose information when adopting healthcare wearables?

The privacy calculus represents the cost/benefit decision or privacy trade-off (Kehr et al., 2015) process that users make to choose whether to disclose their personal information (Wilson & Valacich, 2012). Based on prior research, we conclude that this process imposes consequences towards intentions to use a wearable device (Smith et al., 2011). Thus, we also address:

RQ2: To what extent can one observe the privacy paradox in people's decisions to adopt healthcare wearables?

The privacy paradox characterizes a situation where users contradict expressed concerns regarding privacy (Wilson & Valacich, 2012). In other words, in reference to the privacy calculus, users reveal a net concern about disclosing their personal information while still opting to disclose. Researchers have ascribed this apparent paradox to moderating situational dynamics that override users' general privacy concerns, which results in the decision to disclose (Wilson & Valacich, 2012). To examine whether the privacy paradox manifested in healthcare-related wearables, we sought to measure the moderating effect that perceived health status has on intention to disclose. Perceived health status characterizes a person's assessment towards their illness level and wellness (Kim et al., 2015). Some research has discovered personal perception to moderate privacy/disclosure relationships (e.g., Zhang et al., 2018). Consequently, we postulate a similar moderating effect in our research.

Overall, our research contributes to explaining the privacy paradox's potential to act as a sponsor for people to disclose their private information and accept and use wearable devices. With respect to practice, our study informs manufacturers and healthcare professionals about the privacy/acceptance relationship and encourages them to focus on security matters in both design and use, which can increase consumers' confidence in the effectiveness of wearables and, thus, lead to increased use (Shim et al., 2020).

We structure the paper as follows: in Section 2, we discuss related research in the literature. In Section 3, we present the theoretical background. In Section 4, we propose our research model and hypotheses. In Section 5, we discuss our research methodology. In Section 6, we present and analyze our results. In Section 7, we discuss our findings. Finally, in Section 8, we conclude the paper.

2 Related Work

Based on reviewing privacy-related research literature, Bélanger and Crossler (2011) summarized privacy as the autonomy that people have over their own personal information. Romano and Fjermestad (2007) describe personal information as the authority people have over their personal information regarding how, when, and to what extent it may be distributed. While one may attribute the term "personal information" to static information that organizations generally employ to identify a person such as name, birthdate, and social security number, regarding wearables, we argue the term expands to include biophysical characteristics and personal behavior. When articulating an argument for legislative intervention regarding protection of privacy on the Internet, Clarke (1999) identified four dimensions of privacy that include person, personal behavior, personal communications, and personal data, which all encapsulate the various kinds of data that wearables might capture and synthesize. Clarke (1999) conducted his research because of the potential for consumers to lack "trust in the information society" due to cyberspace's encroachment into individuals' private lives with little or no protections regarding privacy (1999, p. 1).

Privacy's importance in the wearable technology domain has spurred multiple studies. Vitak et al. (2018) researched the impact that concerns about privacy and user-generated data have on how users perceive personal fitness information privacy and observed a positive relationship between a user's concern for privacy and the value a user attributes to fitness data. Although this study and others have made substantial contributions to the privacy and wearable technology domain, they have offered little in identifying the effect that privacy has on technology acceptance.

Gao et al. (2015) performed an empirical study on the adoption of healthcare wearable technologies. In their empirical quest to discover and test antecedents to healthcare wearable device adoption, they discovered that hedonic motivation, functional congruence, social influence, perceived privacy risk, and perceived vulnerability to a health risk influenced fitness device users the most. In contrast, they found that perceived expectancy, self-efficacy, effort expectancy, and perceived health risk severity influenced medical device users the most. Pulipaka (2019) examined the impact that privacy concerns and user perceptions have on healthcare wearable devices and discovered that performance expectancy, effort expectancy, facilitating conditions, and trust strongly predicted device usage intentions. Harper (2016) explored the role that security awareness plays in consumers' decision to adopt IoT devices and found that awareness had a significant influence; however, it did not emerge as the primary factor that led to adoption. Lehto and Lehto (2017) considered the extent to which users perceive their health information as sensitive and their willingness to share it with appropriate parties. They discovered that users in general lacked concerns that wearables collected information about them as they perceived it as unimportant and not private. Consequently, they appeared to base decisions to accept and use wearables not on concerns about privacy; however, the small sample size (i.e., 10 individuals) and the deficiency of statistical analysis in the study prompts concern for further research. Finally, Scott (2020) examined smartwatch acceptance and use in correlation with privacy concerns and found that privacy awareness significantly contributed to smartwatch adoption and that privacy concerns posed a negative influence on intention to use.

The above studies focused on privacy in the wearable technology domain, and four of the six studies specifically targeted healthcare devices. While they have contributed to the conversation on privacy and the factors that influence whether consumers accept and use wearables, a gap regarding the role that the privacy calculus and other factors play in the decision-making process remains. Of the four studies targeting healthcare devices, none specifically examined the role that the privacy calculus and the privacy paradox play in the decision-making process to accept and use healthcare-related wearables. In addition, while Gao et al. (2015) did consider the influence that perceived health threat has on the intention to adopt, none of the acceptance-related studies considered the impact that perceived health status has on the relationship between perceived privacy risk and intention to disclose.

Considering the potential for healthcare-related wearable devices to contribute to improved health and wellbeing, we need to comprehensively consider the effect that privacy has on adoption. We also need to consider the role that one's health status plays in the decision to disclose the information acquired when using the wearable device (Zhang et al., 2018). We focus on filling that gap in this study by investigating

constructs and relationships related to the risk calculus, the privacy calculus, health status, and the privacy paradox in combination with other acceptance-related constructs, in determining how these constructs in aggregate influence (or fail to influence) a person's readiness to use healthcare wearable devices.

3 Theoretical Background

Research has revealed that wearable device consumers do care about their privacy and the necessity for organizations to solicit their informed consent before sharing it with other third-party entities (Anaya et al., 2018). Multiple factors influence privacy concerns, such as privacy experiences, privacy awareness, demographic differences, personality differences, culture, organizational trust, and state-based regulations (Smith et al., 2011). These factors inform how wearable users determine risk regarding divulging their personal information. The perceived sensitivity and vulnerability of one's information and one's confidence level to effectively respond to corresponding threats also play a noteworthy role in determining risk (Kehr et al., 2015). Researchers refer to this threat assessment and the perceived capacity to cope as the risk calculus (Zhang et al., 2018), which the protection motivation theory (PMT) of threat and coping appraisals informs (Li, 2012). Perceived privacy risk (net risks) represents the conclusion of this appraisal process.

However, in addition to the risks associated with disclosing personal data, users also perceive accepting and using healthcare wearables to have benefits. These benefits include fitness activity tracking (Meyer et al., 2015), heart rate monitoring (Muaremi et al., 2013), blood pressure monitoring (Nadeem et al., 2015), and other health-related activities focused on an individual's health and wellbeing. Researchers refer to the process in which one weighs the costs/risks associated with disclosure against these benefits as the privacy calculus (Smith et al., 2011). As we note in Section 1, the privacy calculus expresses the privacy trade-off (Kehr et al., 2015) process that users make to elect whether to disclose their personal information (Wilson & Valacich, 2012). Researchers refer to the risk calculus and privacy calculus theories in combination as the dual-calculus model, which conceptualizes intentions to disclose (Li, 2012).

Privacy theory research is not limited to the protection and disclosure of PII but to personal health information (PHI) as well. Shen (2019) created the content-validated ehealth trust model in response to an investigation regarding the antecedents to trust, structural assurance, and a patient's privacy perspective along with the impact that trust and the privacy calculus (perceived benefit and perceived risk) have on behavior. Zhang et al. (2018) integrated the dual-calculus model and PMT to explore the antecedents to and consequences of PHI privacy concerns in online health communities. In addition to discovering the negative effects that response efficacy and self-efficacy and the positive effects that perceived vulnerability and severity had on privacy concerns, they discovered that perceived health status (PHS) had a moderating effect on the relationship between perceived benefits and the intention to disclose PHI and the relationship between perceived risks and the intention to disclose PHI. They found that PHS weakened the influence that the perceived benefits of informational and emotional support had on PHI disclosure intention and strengthened the influence that perceived risk of health information privacy concerns had on PHI disclosure intention.

Although consumers might often proclaim privacy's importance (Rainie et al., 2013), behavioral observance suggests that many willingly surrender their privacy despite concerns about their personal data (Williams et al., 2016). The reasons why people use wearable devices despite having a risk-oriented intention has been rather allusive (Gerber et al., 2018); however, Williams et al. (2016) recognized five categories of antecedents that contribute to the privacy paradox: 1) education and experience, 2) usability and design, 3) privacy risk salience, 4) social norms, and 5) policies and configurations. Turow et al. (2015) observed that acquiescence to losing autonomy over personal privacy contributes to the privacy paradox.

Various technology acceptance models, the protection motivation theory (PMT), the health belief model (HBM), and various privacy calculus theories inform our research model's theoretical basis. Technology acceptance models focus on forecasting whether individuals will use technology-based systems (Davis et al., 1989). Researchers have developed many models and theories over the past several decades to describe acceptance, three of which have garnered substantial status in technology acceptance research.

First, the technology acceptance model (TAM), which Davis (1986) developed based on Fishbein's and Ajzen's (1975) theory of reasoned action (TRA), hypothesizes that perceived usefulness (PU) and attitude (AT) influences one's behavioral intention (BI) to use a technology, which, in turn, affects their actual usage (AU). Also, both PU and the determinant perceived ease of use (PEOU) influence AT. In turn, other external variables impact PU and PEOS. Davis (1986) excluded the TRA construct subjective norm (SN) from the TAM model due to insufficient knowledge (at the time) about how to suitably place its effects. We note that,

after additionally evaluating and fine-tuning TAM, researchers reduced its constructs to PU, PEOS, and BI (Davis et al., 1989; Venkatesh et al., 2003). Furthermore, in TAM2, a later extension to the original model, researchers reassessed SN as a significant contributor to technology acceptance (Venkatesh & Davis, 2000).

Second, the unified theory of acceptance and use of technology (UTAUT), which Venkatesh et al. (2003) developed, draws on eight previous theories/models: TAM, TRA, the theory of planned behavior (TPB), the motivational model (MM), a model combining TAM with TPB (C-TAM-TPB), innovation diffusion theory (IDT), the model of personal computer utilization (MPCU), and social cognitive theory (SCT). In this way, the model emphasizes that performance expectancy (PE), effort expectancy (EE), and social influence (SI) inform BI and, furthermore, that facilitating conditions (FC) and BI inform AU. UTAUT also posits that gender (G), age (AGE), experience (EX), and voluntariness of use (VU) moderate all relationships except for the relationship between BI and AU. The authors obtained significant findings that resulted in an adjusted R^2 of 69 percent for their original test of the model (based on data from four organizations) and 70 percent for subsequent testing (based on data from two new organizations) (the authors reported both findings in the same paper), which demonstrates a significant increase in performance over the individual contributing models.

Third, the extended UTAUT model (UTAUT2), which Venkatesh et al. (2012) developed, improves on the original UTAUT with three new constructs: hedonic motivation (HM), price value (PV), and habit (HT). The authors condensed the moderators to G, AGE, and EX (i.e., they removed VU from the model). The outcome exhibited an increase in explained variance in regards to behavioral intention (74% compared to 56% for UTAUT) and actual technology use (52% compared to 40% for UTAUT). We used this latter extended model to inform our research model.

Often, threats associated with a technology's adoption influence people's decision to choose it (Gao et al., 2015). Protection motivation theory (PMT) addresses this phenomenon by explaining one's ability to cope and respond to a threat (Woon et al., 2005). A person's response is based on the net effect of the person's threat appraisal and coping appraisal. In the information systems (IS) context, PMT highlights threats to a person's wellbeing resulting from using technology and the person's willingness to adopt technology or technology-related practices and processes (Gao et al., 2015). We considered PMT in its application towards decisions to disclose one's private information.

4 Research Model

Based on the theoretical background, our proposed research model (see Figure 2) depicts factors that we hypothesize to impact whether individuals will adopt and use healthcare-related wearables with a particular emphasis on the risk assessment (risk calculus), the balance between the risks and benefits of disclosure, and their impact on a user's intention to disclose (privacy calculus). The model also depicts the moderating effect that perceived health status (perceived health vulnerability and perceived health severity) has on the relationship between perceived privacy and intention to disclose (privacy paradox). Overall, the model encompasses 16 different constructs (see Table 1). Among them include perceived threat vulnerability (PTV), perceived threat severity (PTS), response efficacy (REF), task self-efficacy (SEF), perceived privacy risk (PPR), hedonic motivation (HMO), performance expectancy (PEX), effort expectancy (EEX), social influence (SIN), technology self-efficacy (TSE), functional congruence (FCG), perceived health status (PHS), intention to disclose (ITD), perceived health vulnerability (PHVU), perceived health severity (PHSE), and intention to adopt (ITA) healthcare wearable devices. Our model extends Gao et al.'s (2015) conceptual model, which they established to review factors related to adopting healthcare wearable devices, and Zhang et al.'s (2018) conceptual model, which they established to review factors that impact health information-related privacy concerns.

Adopted from PMT, perceived threat vulnerability (PTV) refers to the degree to which individuals assess themselves as vulnerable to succumbing to privacy threats (Zhang et al., 2018). Higher PTV will result in higher concern for risks to privacy (Zhang et al., 2018). Thus, we hypothesize that:

H1: Perceived threat vulnerability positively relates to an individual's overall state of perceived privacy risk in the healthcare wearables domain.

Adopted from PMT, perceived threat severity (PTS) refers to the degree to which individuals assess the consequences from succumbing to privacy threats as severe (Zhang et al., 2018). Higher PTS will result in higher concern for risks to privacy (Zhang et al., 2018). Thus, we hypothesize that:

H2: Perceived threat severity positively relates to an individual's overall state of perceived privacy risk in the healthcare wearables domain.

Adopted from PMT, response efficacy (REF) refers to the degree to which individuals assess their current protective measures to prevent themselves from succumbing to privacy threats as effective (Zhang et al., 2018). Higher REF will result in lower concern regarding risks to privacy (Zhang et al., 2018). Thus, we hypothesize that:

H3: Response efficacy negatively relates to an individual's overall state of perceived privacy risk in the healthcare wearables domain.

Adopted from PMT, task self-efficacy (SEF) refers to the degree to which individuals assess themselves as able to successfully implement suitable tasks to respond to privacy threats (Zhang et al., 2018). Higher SEF will result in lower concern regarding risks to privacy (Zhang et al., 2018). Thus, we hypothesize that:

H4: Task self-efficacy negatively relates to an individual's overall state of perceived privacy risk in the healthcare wearables domain.

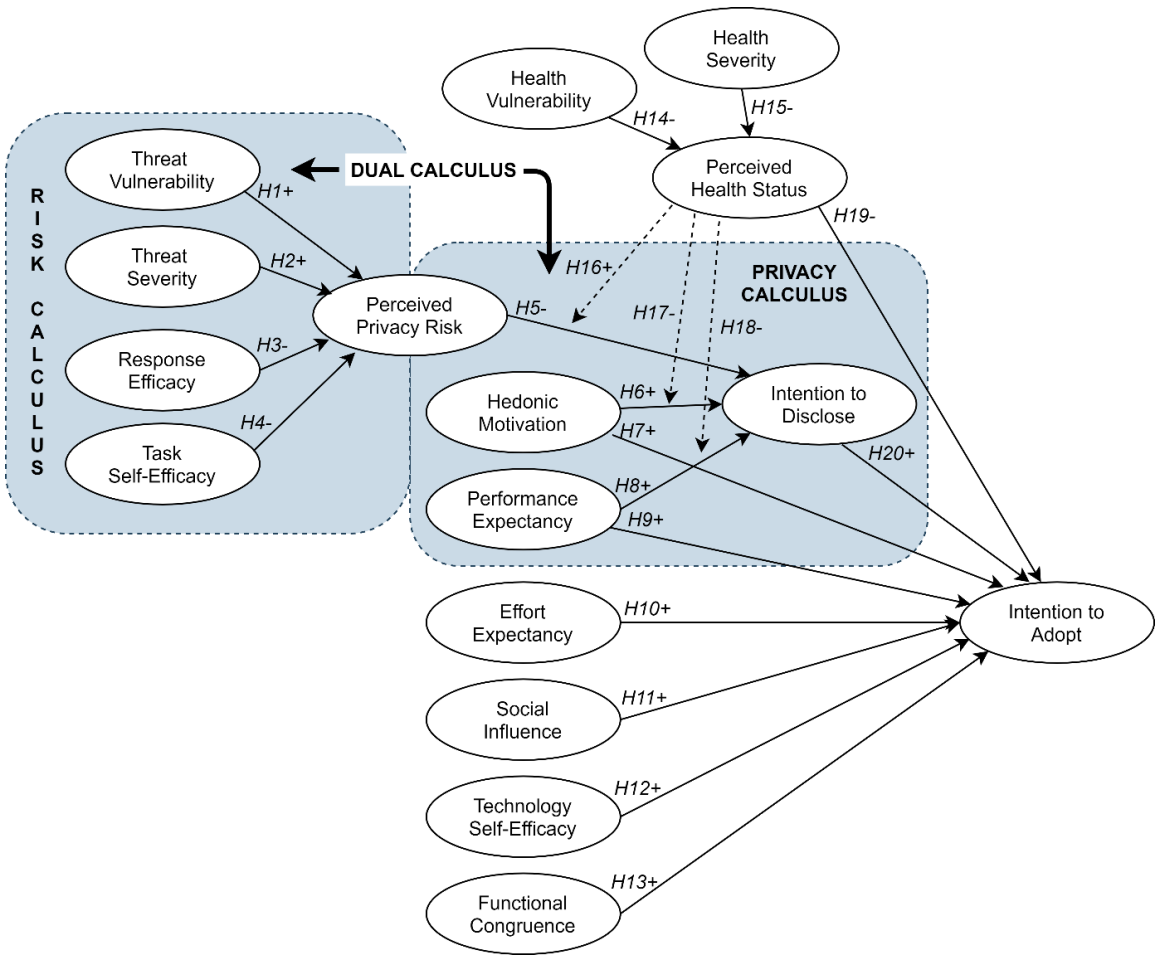

Figure 2. Research Model (Adapted from Zhang et al., 2018; Gao et al., 2015)

Perceived privacy risk (PPR) measures the privacy risk that an individual perceives in regards to using a wearable device. PPR rests on four dimensions of privacy concerns: collection, errors, secondary use, and unauthorized access to private information (Smith et al., 2011). Higher PPR will result in a lower intention to disclose private information as reflected in a user's reluctance to adopt healthcare wearables (Gao et al., 2015). Thus, we hypothesize that:

H5: Perceived privacy risk negatively relates to an individual's intention to disclose privacy information in the healthcare wearables domain.

Adopted from UTAUT2, hedonic motivation (HMO) refers to the intrinsic motivation that users experience (Venkatesh et al., 2012). Intrinsic motivation relates to the pleasure someone experiences from using a wearable device (Brown, 2005). Higher HMO will result in a higher intention to disclose private information and a higher intention to adopt healthcare wearables (Gao et al., 2015). Thus, we hypothesize that:

H6: Hedonic motivation positively relates to an individual's intention to disclose privacy information in the healthcare wearables domain.

H7: Hedonic motivation positively relates to an individual's intention to adopt healthcare wearables.

Adopted from UTAUT, performance expectancy (PEX) refers to how much benefit users expect to gain from using a wearable device (Venkatesh et al., 2003). Higher PEX will result in a higher intention to disclose private information and a higher intention to adopt healthcare wearables (Gao et al., 2015). Thus, we hypothesize that:

H8: Performance expectancy positively relates to an individual's intention to disclose privacy information in the realm of healthcare wearables.

H9: Performance expectancy positively relates to an individual's intention to adopt healthcare wearables.

Adopted from UTAUT, effort expectancy (EEX) refers to a user's perception of the complexity and ease of use of a wearable device (Venkatesh et al., 2003). Higher EEX will result in a higher intention to adopt healthcare wearables (Gao et al., 2015). Thus, we hypothesize that:

H10: Effort expectancy positively relates to an individual's intention to adopt healthcare wearables.

Table 1. Model Variables

Latent Variable	Name	Definition
PTV	Perceived threat vulnerability	Vulnerability to succumb to privacy threats (Zhang et al., 2018).
PTS	Perceived threat severity	Severity of consequences due to succumbing to privacy threats (Zhang et al., 2018).
REF	Response efficacy	Effectiveness of current measures to prevent succumbing to privacy threats (Zhang et al., 2018).
SEF	Task self-efficacy	Ability to implement suitable tasks essential to responding to privacy threats (Zhang et al., 2018).
PPR	Perceived privacy risk	Measurable representation of the privacy risk perceived (Smith et al., 2011).
HMO	Hedonic motivation	Intrinsic motivation experienced (Venkatesh et al., 2012).
PEX	Performance expectancy	Degree of benefit expected (Venkatesh et al., 2003).
EEX	Effort expectancy	Level of effort regarding ease of use/complexity expected (Venkatesh et al., 2003).
SIN	Social influence	Perceived emphasis of others deemed important regarding use (Venkatesh et al., 2003).
TSE	Technology self-efficacy	Perception or belief regarding ability to use particular functions (Gao et al., 2015).
FCG	Functional congruence	Perceived appropriateness of device regarding function and needs (Gao et al., 2015).
PHVU	Perceived health vulnerability	Perception regarding likelihood of succumbing to health threat(s) (Gao et al., 2015).
PHSE	Perceived health severity	Perception regarding extant of health threat(s) responded to (Gao et al., 2015).
PHS	Perceived health status	Perception of illness and wellness (Kim et al., 2015)
ITD	Intention to disclose	Intentions to disclose private information as required (Zhang et al., 2018).
ITA	Intention to adopt	Intentions to adopt a healthcare wearable device (Gao et al., 2015).

Adopted from UTAUT, social influence (SIN) refers to the perceived emphasis of others, who are deemed important to a user, regarding the use of a wearable device (Venkatesh et al., 2003). Higher SIN will result in a higher intention to adopt healthcare wearables (Gao et al., 2015). Thus, we hypothesize that:

H11: Social influence positively relates to an individual's intention to adopt healthcare wearables.

Technology self-efficacy (TSE) refers to the degree to which users perceive or believe themselves as able to use a wearable device's particular functions (Gao et al., 2015). Although researchers dropped TSE from the UTAUT model in regards to general technology acceptance, they have confirmed that it impacts one's intention to adopt emerging health technologies (Sun et al., 2013). Thus, we hypothesize that:

H12: Technology self-efficacy positively relates to an individual's intention to adopt healthcare wearables.

Adapted from self-congruency theory (Huber et al., 2010), functional congruence (FCG) captures the degree to which users perceive a wearable device as appropriate to satisfy their expectations in regards to their functional and basic product-related needs (Gao et al., 2015; Wenling et al., 2015). In contrast to PEX, which refers to the degree to which individuals perceive a device as able to fulfill its specified purpose at a basic level, FCG captures the device's quality in aggregate (i.e., how comfortable one finds it to wear, its durability, and how acceptable one finds its price) (Gao et al., 2015). In other words, although the wearable device may perform as expected (PEX), it must also satisfy practical and applicable expectations given how a user uses it. Thus, we hypothesize that:

H13: Functional congruence positively relates to an individual's intention to adopt healthcare wearables.

Informed by PMT, perceived health vulnerability (PHVU) refers to the degree to which users perceive themselves as likely to succumb to health threat(s) that a wearable device directly or indirectly addresses (Gao et al., 2015). Higher PHVU will result in a lower perceived health status. Thus, we hypothesize that:

H14: Perceived health vulnerability negatively relates to an individual's overall state of perceived health status in the healthcare wearables domain.

Informed by PMT, perceived health severity (PHSE) refers to the user's perception regarding the austerity of the health threat(s) that a wearable device directly or indirectly addresses (Gao et al., 2015). Higher PHSE will result in a lower perceived health status. Thus, we hypothesize that:

H15: Perceived health severity negatively relates to an individual's overall state of perceived health status in the healthcare wearables domain.

Perceived health status (PHS) refers to the degree to which individuals perceive themselves as healthy (Kim et al., 2015), which research has found to moderate privacy/disclosure relationships (Zhang et al., 2018). Therefore, we postulate a similar moderating effect in the current model. Informed by HBM (Janz & Becker, 1984), which emphasizes that increases in perceived risk inspire self-protective behavior (Deng & Liu, 2017), we hypothesize that PHS is an antecedent to intention to adopt, which emphasizes that higher PHS (better health) has a negative impact on whether users adopt healthcare wearables. Thus, we hypothesize that:

H16: Perceived privacy risk has a stronger influence on intention to disclose when an individual has a high perceived health status.

H17: Hedonic motivation has a weaker influence on intention to disclose when an individual has a high perceived health status.

H18: Performance expectancy has a weaker influence on intention to disclose when an individual has a high perceived health status.

H19: Perceived health status negatively relates to an individual's intention to adopt healthcare wearables.

Intention to disclose (ITD) refers to a user's intention to disclose private information as required when using a healthcare wearable device (Zhang et al., 2018). Higher ITD will result in a higher intention to adopt healthcare wearables. Thus, we hypothesize that:

H20: Intention to disclose positively relates to an individual's intention to adopt healthcare wearables.

Intention to adopt healthcare wearables (ITA) characterizes a user's intention to adopt a healthcare wearable device (Gao et al., 2015).

5 Research Methodology

5.1 Survey Instrument

The instrument comprised 58 measurements: 52 Likert-based questions, one interval-based measurement, and five demographics (see Appendix A). We measured items on a seven-point Likert scale where one represented "strongly disagree" and seven represented "strongly agree" (Dittrich et al., 2007) except for PHS, which we measured based on one question that asked whether the participant perceived their health to be "very poor", "poor", "fair", "good", or "excellent". Research has observed self-rated general health assessments to demonstrate noteworthy performance and to represent an acceptable alternative to multi-item measurements (Zhang et al., 2018). Every question measured a specific model construct that past research has validated and verified. We needed to ensure that each question stood on its own without influence from other questions in order to circumvent common methods bias, a threat to construct validity (Straub et al., 2004). We also collected vital demographic information, such as gender, age range, education, and whether the wearable was recommended, mandated, or neither.

5.2 Data Collection

For our survey, we targeted individuals over 18 years old who had used, did use, or had considered using healthcare wearable devices. We did not target any specific demographics. In addition, we did not collect any personally identifiable information in order to ensure participants' anonymity. We disseminated the survey via social media, email, and related discussion board forums such as Facebook, Twitter, LinkedIn, Reddit, and Pinterest. We used Qualtrics to build, test, and distribute the survey to the target audiences.

We focused on querying a large enough sample to ensure we could generalize our findings to the general population (Roberts, 2012). As such, we sought 200 responses at minimum, which is sufficient for PLS-SEM analysis when estimating models with a maximum of ten exogenous variables pointing to a single endogenous variable and seeking a statistical power of 80 percent, a significance level of 0.01, and a minimum coefficient of determination (R_2) of 0.100 (Hair et al., 2017). We used IBM SPSS to handle missing values and for outlier analyses. For missing values, we used mean replacement provided that the number of missing values did not exceed the recommended threshold (i.e., 5%) (Hair et al., 2017). We considered outliers for removal only if we could identify a plausible explanation for them (e.g., entry errors) (Hair et al., 2017).

5.3 Data Analysis

We selected the partial least squares structural equation modeling (PLS-SEM) method for this research effort due to its recognized ability towards exploratory research in the social science sciences and for its resilience towards estimating causative relationships between constructs (Hair et al., 2017). In contrast, confirmation-based research often uses covariance-based SEM (CB-SEM) to test existing theories. CB-SEM favors large sample sizes and normally distributed data, whereas PLS-SEM can handle smaller sample sizes and makes no assumptions towards data distribution (Wong, 2013). We selected SmartPLS version 3.3.3 (Ringle et al., 2015) as the tool for PLS-SEM estimation due to its acceptance among the academic community (Wong, 2019) and for its graphical interface, ease of use, and efficiency in estimation.

6 Results

We collected 225 responses in total. Three of the cases included missing values for all indicators for one or more constructs. We eliminated these cases due to our inability to measure specific constructs for those specific cases. For the 222 remaining cases, we identified one case with two missing values (separate constructs) (4% of the cases) and 11 cases with one missing value each (2% of each case). As such, the entire dataset had 13 missing values (0.11% of total). The maximum number of missing values for any particular indicator was 0.9 percent. Consequently, we chose mean replacement as the preferred method for missing value replacement during PLS-SEM analysis since 0.9 percent falls well below the

recommended 5 percent threshold (Hair et al., 2017). We identified outliers for 22 of the 53 indicators. However, we did not adjust or delete these outliers since we had no plausible explanation for them (e.g., entry errors). The fact that our model estimation completed in three iterations, significantly less than the 300 iterations configured as the stop criterion (Wong, 2019), later reinforced that decision. Furthermore, it confirmed the resultant sample size (i.e., 222) (Hair et al., 2017). Table 2 exhibits the central tendency and dispersion statistical measures for the demographic-related data. Figures 3 and 4 graphically represent the data's distribution.

Table 2. Statistical Measures of Central Tendency and Dispersion: Demographics

Demographic	Description	N	Min	Max	Mean	StdDev
USE	Use recommended, mandated, or neither	222	1	3	2.78	0.617
CHC	Current chronic health condition	221	1	2	1.77	0.419
GDR	Gender	221	1	2	1.60	0.492
AGE	Age	220	1	6	3.17	1.347
EDU	Education	222	2	7	4.61	1.484

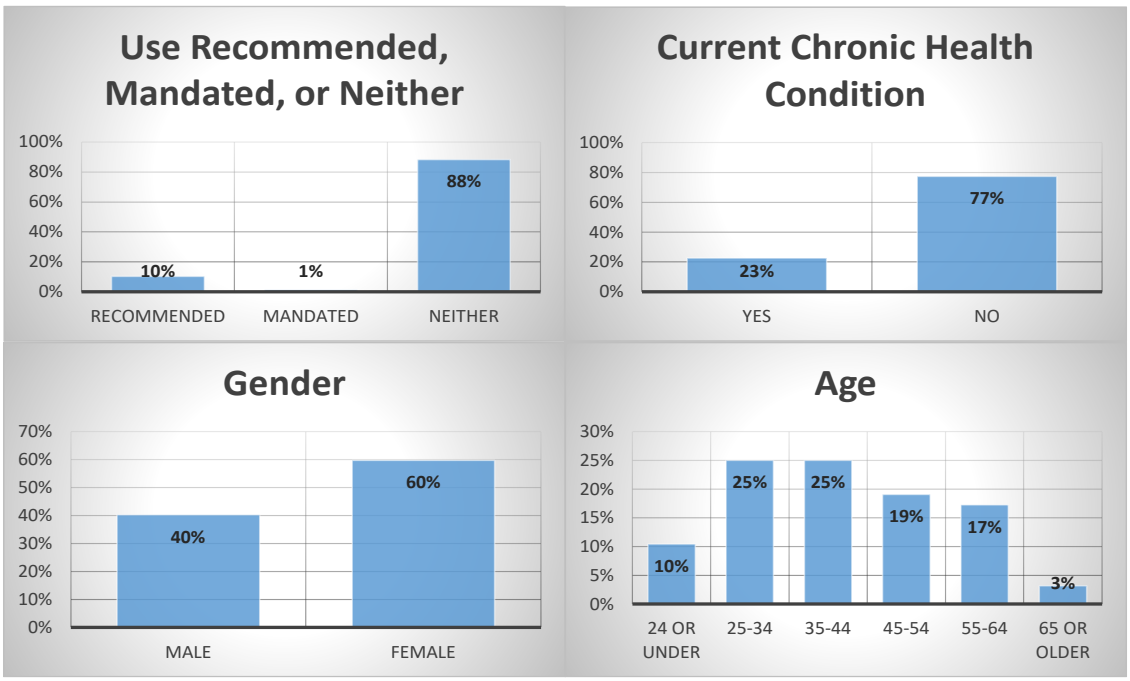

Figure 3. Sample Distribution: USE, CHC, GDR, and AGE

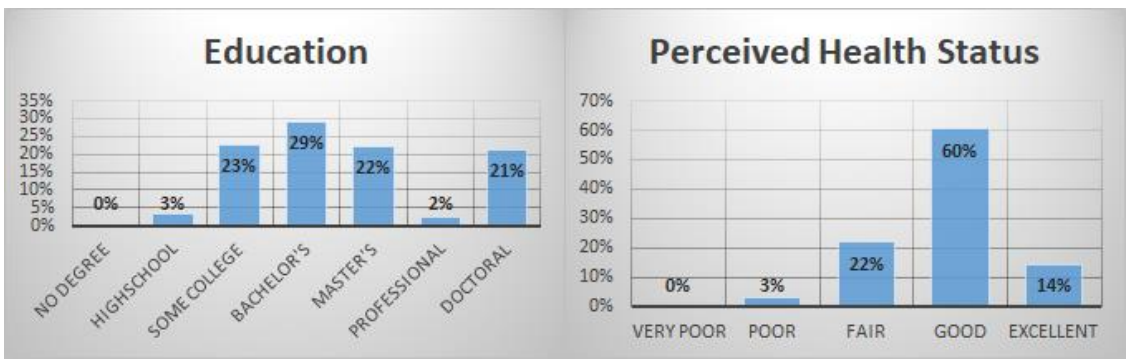

Figure 4. Sample Distribution: EDU, PHS

Table 3 exhibits the central tendency and dispersion statistical measures for the measurement instrument. Except for PHS, all construct measurements involved multiple indicators based on a seven-point Likert scale with one representing “strongly disagree” and seven representing “strongly agree” (Dittrich et al., 2007). We measured the construct PHS based on one question that asked participants whether they perceived their health to be “very poor”, “poor”, “fair”, “good”, or “excellent. The statistical measures in Table 3 include the latent variable and corresponding indicators, sample size (which varied due to missing values), minimum and maximum values, mean, standard deviation, and skewness and kurtosis.

Table 3. Statistical Measures of Central Tendency and Dispersion: Measurement Instrument

Latent variable	Indicator	N	Min	Max	Mean	StdDev	Skewness		Kurtosis	
							Statistic	StdErr	Statistic	StdErr
PTV	PTV1	222	1	7	4.14	1.854	-0.169	0.163	-1.143	0.325
	PTV2	222	1	7	3.97	1.780	0.007	0.163	-1.087	0.325
	PTV3	222	1	7	4.85	1.732	-0.737	0.163	-0.398	0.325
	PTV4	222	1	7	4.36	1.821	-0.292	0.163	-1.064	0.325
PTS	PTS1	222	1	7	3.75	1.782	0.183	0.163	-1.037	0.325
	PTS2	222	1	7	4.04	1.843	-0.012	0.163	-1.217	0.325
	PTS3	222	1	7	4.20	1.840	-0.135	0.163	-1.180	0.325
	PTS4	222	1	7	4.40	1.902	-0.335	0.163	-1.185	0.325
REF	REF1	222	1	7	4.13	1.545	-0.407	0.163	-0.580	0.325
	REF2	222	1	7	4.00	1.518	-0.282	0.163	-0.632	0.325
	REF3	222	1	7	4.39	1.508	-0.537	0.163	-0.166	0.325
SEF	SEF1	222	1	7	4.05	1.511	-0.299	0.163	-0.383	0.325
	SEF2	221	1	7	4.12	1.629	-0.377	0.164	-0.820	0.326
	SEF3	222	1	7	4.02	1.625	-0.202	0.163	-0.990	0.325
	SEF4	222	1	7	4.01	1.648	-0.253	0.163	-0.893	0.325
PPR	PPR1	222	1	7	3.55	1.682	0.552	0.163	-0.763	0.325
	PPR2	222	1	7	3.35	1.618	0.425	0.163	-0.564	0.325
	PPR3	222	1	7	4.65	1.811	-0.577	0.163	-0.588	0.325
HMO	HMO1	222	1	7	5.46	1.175	-1.069	0.163	1.770	0.325
	HMO2	222	1	7	5.45	1.209	-1.093	0.163	1.599	0.325
	HMO3	222	1	7	5.16	1.328	-0.820	0.163	0.608	0.325
	HMO4	222	1	7	5.32	1.273	-0.885	0.163	0.692	0.325
PEX	PEX1	221	1	7	5.26	1.312	-0.959	0.164	1.138	0.326
	PEX2	222	1	7	5.60	1.163	-1.115	0.163	1.895	0.325
	PEX3	222	1	7	5.49	1.199	-1.116	0.163	1.621	0.325
EEX	EEX1	222	1	7	5.90	1.059	-1.531	0.163	3.324	0.325
	EEX2	222	1	7	5.82	1.078	-1.276	0.163	2.240	0.325
	EEX3	220	1	7	5.83	1.144	-1.345	0.164	2.109	0.327
	EEX4	222	1	7	5.82	1.106	-1.329	0.163	2.144	0.325
SIN	SIN1	221	1	7	4.24	1.534	-0.379	0.164	-0.327	0.326
	SIN2	221	1	7	4.12	1.491	-0.262	0.164	-0.386	0.326
	SIN3	222	1	7	4.05	1.497	-0.264	0.163	-0.341	0.325
TSE	TSE1	221	1	7	5.71	1.048	-1.408	0.164	3.722	0.326
	TSE2	220	1	7	5.84	0.965	-1.418	0.164	4.651	0.327
	TSE3	222	1	7	5.64	1.156	-1.273	0.163	2.288	0.325

Table 3. Statistical Measures of Central Tendency and Dispersion: Measurement Instrument

FCG	FCG1	222	1	7	5.67	1.019	-1.082	0.163	1.797	0.325
	FCG2	222	1	7	5.07	1.375	-0.776	0.163	0.389	0.325
	FCG3	222	1	7	4.83	1.438	-0.645	0.163	-0.209	0.325
	FCG4	221	1	7	5.41	1.246	-1.248	0.164	1.758	0.326
PHVU	PHVU1	222	1	7	3.13	1.662	0.579	0.163	-0.651	0.325
	PHVU2	222	1	7	3.11	1.617	0.619	0.163	-0.569	0.325
	PHVU3	222	1	7	3.45	1.711	0.323	0.163	-1.010	0.325
PHSE	PHSE1	222	1	7	3.87	1.655	-0.050	0.163	-0.866	0.325
	PHSE2	222	1	7	3.97	1.683	-0.181	0.163	-0.904	0.325
	PHSE3	221	1	7	4.04	1.738	-0.199	0.164	-1.015	0.326
ITD	ITD1	222	1	7	4.92	1.743	-0.947	0.163	-0.262	0.325
	ITD2	221	1	7	4.71	1.851	-0.732	0.164	-0.705	0.326
	ITD3	222	1	7	5.05	1.789	-1.087	0.163	0.033	0.325
ITA	ITA1	222	1	7	5.64	1.466	-1.442	0.163	1.922	0.325
	ITA2	221	1	7	5.11	1.761	-0.839	0.164	-0.311	0.326
	ITA3	222	1	7	5.55	1.515	-1.389	0.163	1.583	0.325
	ITA4	222	1	7	5.02	1.892	-0.907	0.163	-0.393	0.325
PHS	PHS	222	2	5	3.86	0.688	-0.400	0.163	0.373	0.325

Skewness measures asymmetry and Kurtosis measures a distribution's "peakedness" relative to a normal distribution (Hae-Young, 2013, p. 2). Although PLS-SEM makes no assumptions in regards to distribution (Wong, 2013) and can better tolerate concerns of normality (Hair et al., 2017), one still needs to consider its presence during the analysis process (Hair et al., 2017). Researchers consider an absolute skewness value and/or kurtosis value greater than 1 as departure from normality (Hair et al., 2017). Using this criterion, we identified some concerns regarding skewness and kurtosis for some or all indicators for the variables PTV, PTS, HMO, PEX, EEX, TSE, FCG, PHVU, PHSE, ITD, and ITA.

6.1 Measurement Model Testing

Table 4 summarizes the results we obtained from assessing the measurement model's quality, which included tests for convergent validity, internal consistency reliability, and discriminant validity using a 0.05 significance level (alpha) and bias correction (BC) for interval analysis. All loadings, except for three indicators, exceeded the recommended value 0.70 and accounted 50 percent at minimum of the variance regarding the related constructs (Gao et al., 2015). Of the three loadings that fell below, PPR3 and ITA4 measured just under the 0.70 minimum (Hair et al., 2017) at 0.678 and 0.677, respectively, and PTS4 measured significantly under the recommended minimum at 0.443. Table 5 shows measurement model's significance after bootstrapping.

To guarantee adherence to the recommended minimum for loadings, we removed the three indicators with loadings less than 0.70. After doing so, we noted an increase in AVE and internal consistency reliability values, which confirmed our decision (Hair et al., 2017). Figure 5 shows the research model post analysis using SmartPLS (Ringle et al., 2015).

AVE values for all latent variables exceeded the recommended minimum 0.50 (Hair et al., 2017), which confirmed convergent validity. We measured internal consistency against the accepted values 0.60 and 0.70 for Cronbach's alpha and composite reliability (CR), respectively. All model constructs passed, which indicated no concerns with internal consistency (Hair et al., 2017). Finally, we used two heterotrait-monotrait (HTMT) criteria to measure discriminant validity: 1) an HTMT ratio of correlations score below the cutoff of 0.85 (Hair et al., 2020) and 2) an HTMT interval not containing the value of 1 (considering a confidence level of 95%) (Hair et al., 2017; Wong, 2019). We found all constructs to pass both criteria, which confirmed discriminant validity. Referring to Table 5, all tests exhibited significance at the 0.05 level.

Table 4. Measurement Model Test Summary

Latent variable	Indicator	Convergent validity			Internal consistency reliability		Discriminant validity	
		Loadings	Indicator reliability	AVE	Cronbach's alpha	Composite reliability	HTMT	
		> 0.70	> 0.50	> 0.50	> 0.60	> 0.70	< 0.85	HTMT confidence level (BC) does not include 1
PTV	PTV1	0.901	0.812	0.815	0.924	0.946	Yes	Yes
	PTV2	0.921	0.848					
	PTV3	0.885	0.783					
	PTV4	0.902	0.814					
PTS	PTS1	0.938	0.880	0.723	0.851	0.907	Yes	Yes
	PTS2	0.951	0.904					
	PTS3	0.953	0.908					
	PTS4	0.443	0.196					
REF	REF1	0.934	0.872	0.786	0.864	0.916	Yes	Yes
	REF2	0.948	0.899					
	REF3	0.765	0.585					
SEF	SEF1	0.905	0.819	0.860	0.946	0.961	Yes	Yes
	SEF2	0.939	0.882					
	SEF3	0.940	0.884					
	SEF4	0.924	0.854					
PPR	PPR1	0.840	0.706	0.641	0.715	0.841	Yes	Yes
	PPR2	0.870	0.757					
	PPR3	0.678	0.460					
HMO	HMO1	0.952	0.906	0.823	0.927	0.949	Yes	Yes
	HMO2	0.943	0.889					
	HMO3	0.878	0.771					
	HMO4	0.851	0.724					
PEX	PEX1	0.837	0.701	0.793	0.869	0.920	Yes	Yes
	PEX2	0.918	0.843					
	PEX3	0.915	0.837					
EEX	EEX1	0.928	0.861	0.866	0.948	0.963	Yes	Yes
	EEX2	0.950	0.903					
	EEX3	0.907	0.823					
	EEX4	0.936	0.876					
SIN	SIN1	0.952	0.906	0.931	0.963	0.976	Yes	Yes
	SIN2	0.973	0.947					
	SIN3	0.969	0.939					
TSE	TSE1	0.930	0.865	0.785	0.864	0.916	Yes	Yes
	TSE2	0.910	0.828					
	TSE3	0.814	0.663					
FCG	FCG1	0.850	0.723	0.613	0.790	0.863	Yes	Yes

Table 4. Measurement Model Test Summary

	FCG2	0.783	0.613					
	FCG3	0.740	0.548					
	FCG4	0.755	0.570					
PHVU	PHVU1	0.924	0.854	0.859	0.918	0.948	Yes	Yes
	PHVU2	0.950	0.903					
	PHVU3	0.906	0.821					
PHSE	PHSE1	0.955	0.912	0.942	0.970	0.980	Yes	Yes
	PHSE2	0.987	0.974					
	PHSE3	0.970	0.941					
PHS	PHS1	1.000	1.000	1.000	1.000	1.000	Yes	Yes
ITD	ITD1	0.883	0.780	0.790	0.867	0.919	Yes	Yes
	ITD2	0.907	0.823					
	ITD3	0.875	0.766					
ITA	ITA1	0.930	0.865	0.693	0.847	0.899	Yes	Yes
	ITA2	0.895	0.801					
	ITA3	0.806	0.650					
	ITA4	0.677	0.458					

Table 5. Measurement Model Significance

Latent variable	Indicator	Convergent Validity				Internal consistency reliability			
		Loadings		AVE		Cronbach's alpha		Composite reliability	
		Confidence interval (BC)	P-value	Confidence interval (BC)	P-value	Confidence interval (BC)	p-value	Confidence interval (BC)	p-value
PTV	PTV1	(0.851, 0.937)	0.000	(0.772, 0.855)	0.000	(0.902, 0.944)	0.000	(0.931, 0.959)	0.000
	PTV2	(0.895, 0.942)	0.000						
	PTV3	(0.844, 0.917)	0.000						
	PTV4	(0.868, 0.928)	0.000						
PTS	PTS1	(0.913, 0.956)	0.000	(0.687, 0.764)	0.000	(0.809, 0.887)	0.000	(0.886, 0.926)	0.000
	PTS2	(0.930, 0.969)	0.000						
	PTS3	(0.937, 0.965)	0.000						
	PTS4	(0.255, 0.596)	0.000						
REF	REF1	(0.907, 0.953)	0.000	(0.727, 0.834)	0.000	(0.814, 0.900)	0.000	(0.887, 0.938)	0.000
	REF2	(0.926, 0.964)	0.000						
	REF3	(0.652, 0.839)	0.000						
SEF	SEF1	(0.868, 0.930)	0.000	(0.819, 0.893)	0.000	(0.926, 0.960)	0.000	(0.948, 0.971)	0.000
	SEF2	(0.915, 0.956)	0.000						
	SEF3	(0.917, 0.957)	0.000						
	SEF4	(0.869, 0.955)	0.000						
PPR	PPR1	(0.770, 0.886)	0.000	(0.582, 0.693)	0.000	(0.631, 0.775)	0.000	(0.803, 0.871)	0.000
	PPR2	(0.820, 0.901)	0.000						
	PPR3	(0.564, 0.764)	0.000						
HMO	HMO1	(0.930, 0.966)	0.000	(0.771, 0.867)	0.000	(0.899, 0.948)	0.000	(0.931, 0.963)	0.000
	HMO2	(0.917, 0.960)	0.000						

Table 5. Measurement Model Significance

	HMO3	(0.822, 0.915)	0.000						
	HMO4	(0.777, 0.904)	0.000						
PEX	PEX1	(0.742, 0.893)	0.000	(0.725, 0.848)	0.000	(0.808, 0.910)	0.000	(0.887, 0.944)	0.000
	PEX2	(0.867, 0.947)	0.000						
	PEX3	(0.878, 0.940)	0.000						
EEX	EEX1	(0.882, 0.956)	0.000	(0.817, 0.905)	0.000	(0.926, 0.965)	0.000	(0.947, 0.975)	0.000
	EEX2	(0.916, 0.969)	0.000						
	EEX3	(0.839, 0.945)	0.000						
	EEX4	(0.894, 0.961)	0.000						
SIN	SIN1	(0.922, 0.971)	0.000	(0.898, 0.953)	0.000	(0.947, 0.976)	0.000	(0.963, 0.984)	0.000
	SIN2	(0.952, 0.984)	0.000						
	SIN3	(0.952, 0.980)	0.000						
TSE	TSE1	(0.885, 0.956)	0.000	(0.699, 0.856)	0.000	(0.788, 0.916)	0.000	(0.873, 0.947)	0.000
	TSE2	(0.850, 0.947)	0.000						
	TSE3	(0.644, 0.908)	0.000						
FCG	FCG1	(0.765, 0.917)	0.000	(0.542, 0.690)	0.000	(0.719, 0.847)	0.000	(0.825, 0.901)	0.000
	FCG2	(0.665, 0.864)	0.000						
	FCG3	(0.572, 0.832)	0.000						
	FCG4	(0.605, 0.850)	0.000						
PHVU	PHVU1	(0.805, 0.964)	0.000	(0.796, 0.908)	0.000	(0.881, 0.945)	0.000	(0.923, 0.968)	0.000
	PHVU2	(0.874, 0.972)	0.000						
	PHVU3	(0.789, 0.964)	0.000						
PHSE	PHSE1	(0.355, 0.986)	0.000	(0.812, 0.966)	0.000	(0.955, 0.980)	0.000	(0.930, 0.989)	0.000
	PHSE2	(0.854, 0.994)	0.000						
	PHSE3	(0.839, 0.998)	0.000						
PHS	PHS	(1.000, 1.000)	0.000	(1.000, 1.000)	0.000	(1.000, 1.000)	NA	(1.000, 1.000)	NA
ITD	ITD1	(0.818, 0.924)	0.000	(0.724, 0.847)	0.000	(0.811, 0.910)	0.000	(0.887, 0.943)	0.000
	ITD2	(0.867, 0.938)	0.000						
	ITD3	(0.809, 0.916)	0.000						
ITA	ITA1	(0.906, 0.948)	0.000	(0.628, 0.751)	0.000	(0.791, 0.887)	0.000	(0.868, 0.923)	0.000
	ITA2	(0.859, 0.921)	0.000						
	ITA3	(0.689, 0.875)	0.000						
	ITA4	(0.549, 0.778)	0.000						

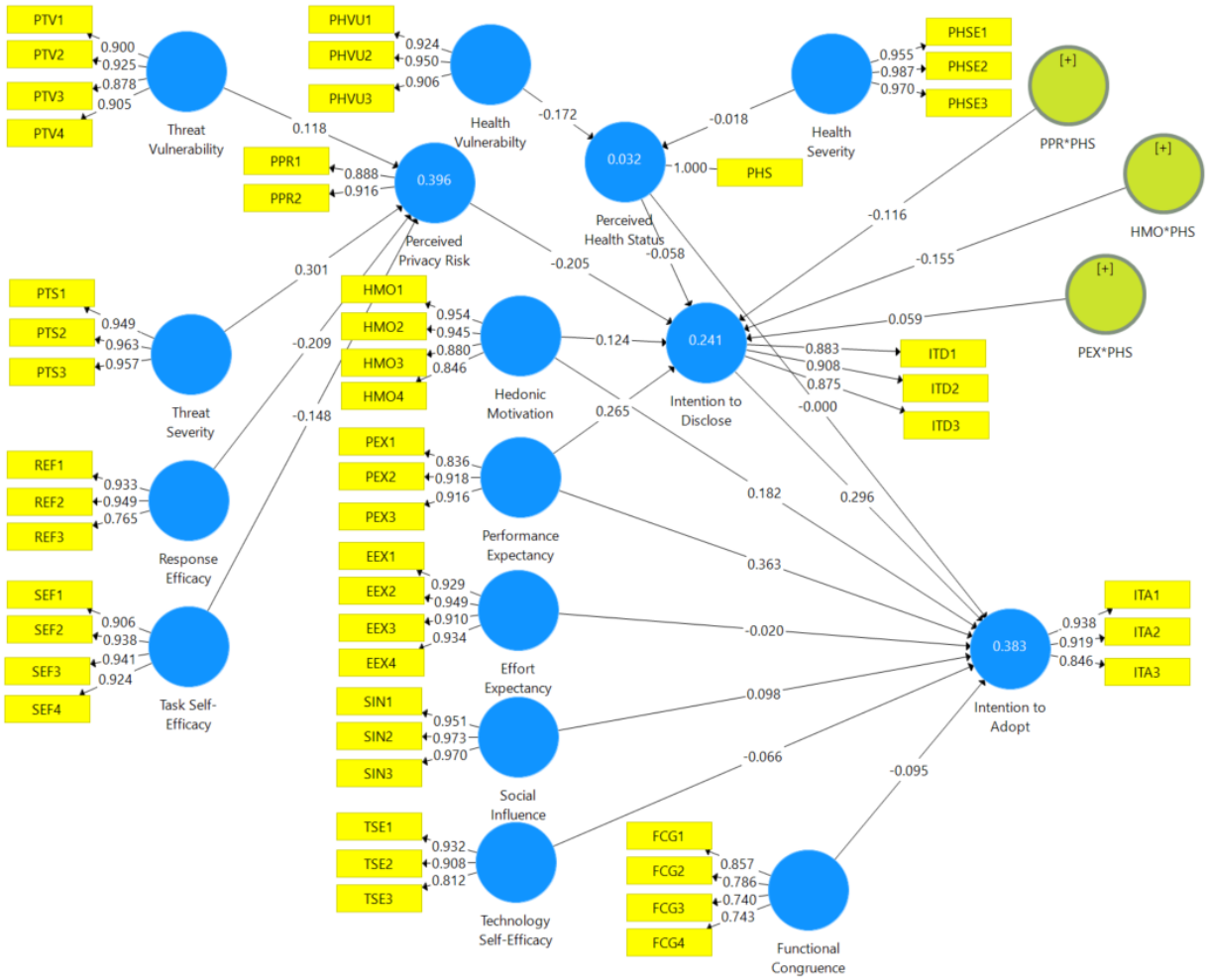

Figure 5. Research Model (Loadings > 0.70)

6.2 Structural Model Testing

We estimated the model using the PLS algorithm with complete bootstrapping using the bias-corrected confidence interval method, two-tailed test, 5,000 subsamples, and mean replacement for missing values. Table 6 summarizes the model estimation results pertaining specifically to the endogenous variables. We note the explained variances of 39.6 percent (moderate) for PPR, 3.2 percent (very weak) for PHS, 24.1 percent (weak) for ITD, and 38.3 percent (moderate) for ITA (Hair et al., 2011); however, the significance level (p-value) for PHS was notably larger than 0.05, which casts doubt on the explained variance. We used the blindfolding method with a 7 omission distance (OD) to calculate Stone-Geisser's Q^2, which determines a model's predictive relevance (Wong, 2019). We identified a weak predictive relevance for PHS, better than moderate relevance for PPR and ITA, and moderate relevance for ITD.

Table 6. Endogenous Variable Summary

Endogenous latent variable	Coefficient of determination (R^2)			R2 adjusted			Predictive relevance Q2
	Value	Confidence interval (BC)	P-value	Value	Confidence interval (BC)	P-value	
PPR	0.396	(0.285, 0.485)	0.000	0.385	(0.272, 0.476)	0.000	0.306
PHS	0.032	(0.004, 0.084)	0.227	0.023	(-0.005, 0.076)	0.385	0.014
ITD	0.241	(0.116, 0.336)	0.000	0.216	(0.088, 0.315)	0.000	0.170
ITA	0.383	(0.203, 0.511)	0.000	0.360	(0.173, 0.492)	0.000	0.287

6.2.1 Moderator Analysis

H16, H17, and H18 hypothesized that PHS had a moderating effect on the relationships between the exogenous variables PPR, HMO, and PEX and the endogenous variable ITD. Regarding moderator analysis, the path coefficient represents the interaction term. Using the two-stage approach for creating the interaction terms, the graphs in Figures 6, 7, and 8 represent the results of the slope analysis of the moderating effect of PHS on the exogenous/endogenous relationships. The x-axis signifies the exogenous variable and the y-axis signifies the ITD endogenous variable. The red line signifies the effect of PHS at mean, the blue line at -1 standard deviation (SD), and the green line at +1 SD.

Regarding PPR (see Figure 6), which we discovered to normally have a negative impact on ITD, we found a decrease in the negative influence that it had on ITD with a lower PHS (blue line) and an increase in the negative influence that PPR had on ITD with a higher PHS (green line). The interaction term path coefficient of -0.116 reflects this finding and supports H16. When analyzing moderators, a 0.005, 0.01, and 0.25 effect size (f^2) constitutes a small, medium, and large effect, respectively (Hair et al., 2017; Kenny, 2018). Accordingly, we note that PHS had a somewhat large effect (0.014) on the PPR→ITD relationship, though the p-value 0.116 means it fell just outside the bounds for statistical significance at the 10 percent level.

Regarding HMO (see Figure 7), which we discovered to normally have a positive influence on ITD, we found a significant increase in the positive impact that it had on ITD with a lower PHS (blue line) and a decrease in the positive impact with a higher PHS (green line). The interaction term of -0.155 reflects this finding and supports H17. We found that PHS had a somewhat large effect (0.021) on the HMO→ITD relationship.

Regarding PEX (see Figure 8), which we discovered normally has a positive impact on ITD, we found an increase in the positive influence that it had on ITD with a lower PHS (blue line) and a decrease in the positive influence with a higher PHS (green line). The interaction term of 0.059 reflects this finding and supports H18. However, since PHS had a very small effect (0.003) on the PEX→ITD relationship, we determined that it lacked significance and, thus, we did not find support for H18.

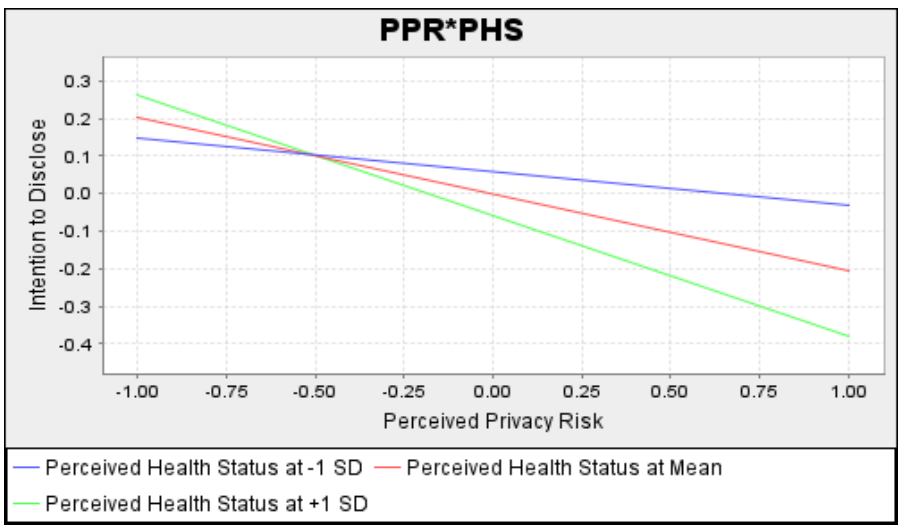

Figure 6. Moderating Effect that PHS had on PPR→ITD

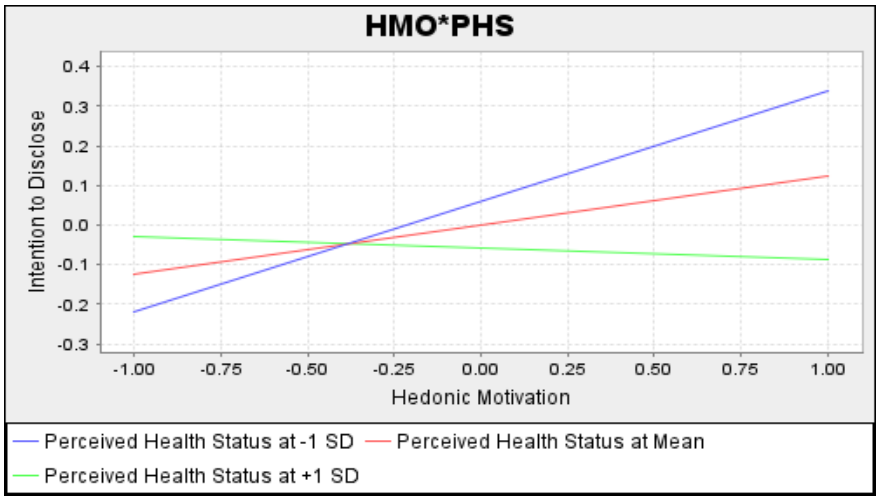

Figure 7. Moderating Effect that PHS Had on HMO→ITD

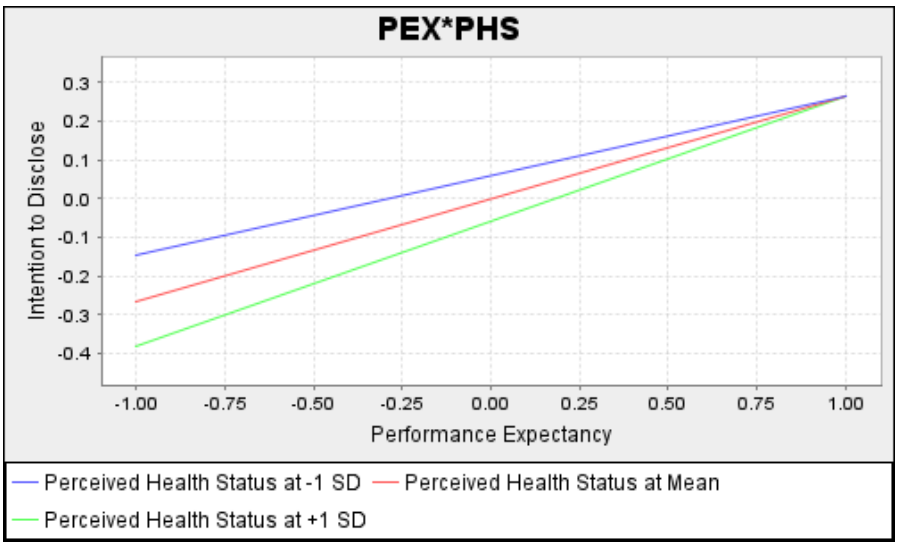

Figure 8. Moderating Effect that PHS had on PEX→ITD

6.2.2 Structural Model Test Summary

Figure 9 represents the final model after testing. We show strongly supported relationships/hypotheses in black, reservedly confirmed relationships/hypotheses in purple, and notably insignificant relationships/hypotheses in red.

Sorted by hypotheses, Table 7 summarizes the effect that the exogenous variables had on their corresponding endogenous variables (including the moderating effect of PHS). Considering the VIF values did not surpass 5.0, we note that multicollinearity did not pose a concern for all hypothesized relationships (Hair et al., 2013). Based on path coefficients and significance, we found support for H2, H3, H5, H8, H9, and H20 at the 0.01 alpha level (***); for H7, H14, and H17 at the 0.05 alpha level (**); and for H4 at the 0.10 alpha level (*). We did not find support for H6, H11, and H16 (0.105, 0.114, and 0.116 alpha levels, respectively). H1 somewhat surpassed acceptable significance levels.

We found that H10, H12, H13, H15, H18, and H19 well surpassed acceptable significance levels, which means we failed to deduce any effect in the relationships between latent constructs. Effect size (f^2) signifies the impact that exogenous variables have on endogenous variables with 0.02, 0.15, and 0.35 being criteria for a small, medium, and large impact, respectively (Hair et al., 2013). Of the significant relationships identified, H2, H9, and H20 had a somewhat medium impact, while the others had a somewhat small impact.

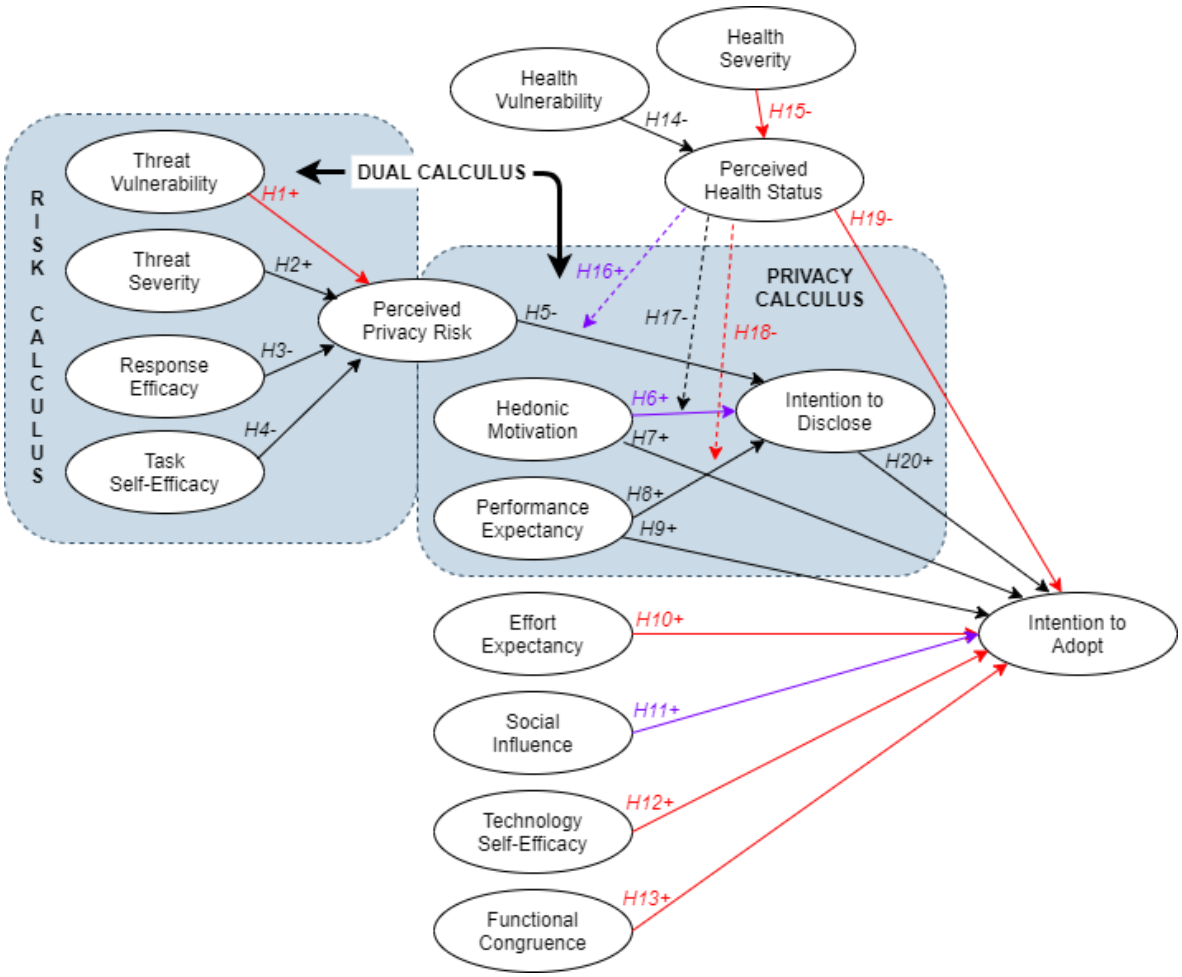

Figure 9. Research Model After Testing

Table 7. Structural Model Test Summary

H	Relationship	VIF < 5.0	Path coefficient	Confidence interval (BC)	p-value		Effect size (f2)
H1+	PTV -> PPR	1.817	0.118	(-0.030, 0.274)	0.135		0.013
H2+	PTS -> PPR	1.375	0.301	(0.187, 0.410)	0.000	***	0.109
H3-	REF -> PPR	2.380	-0.209	(-0.362, -0.049)	0.009	***	0.030
H4-	SEF -> PPR	2.347	-0.148	(-0.312, 0.017)	0.079	*	0.016
H5-	PPR -> ITD	1.112	-0.205	(-0.340, -0.061)	0.004	***	0.050
H6+	HMO -> ITD	1.503	0.124	(-0.023, 0.280)	0.105		0.014
H7+	HMO -> ITA	1.688	0.182	(0.028, 0.349)	0.026	**	0.032
H8+	PEX -> ITD	1.585	0.265	(0.094, 0.417)	0.001	***	0.058
H9+	PEX -> ITA	2.356	0.363	(0.156, 0.560)	0.001	***	0.091
H10+	EEX -> ITA	1.831	-0.020	(-0.170, 0.117)	0.780		0.000

Table 7. Structural Model Test Summary

H11+	SIN -> ITA	1.272	0.098	(-0.024, 0.219)	0.114		0.012
H12+	TSE -> ITA	2.038	-0.066	(-0.257, 0.113)	0.490		0.003
H13+	FCG -> ITA	1.690	-0.095	(-0.253, 0.023)	0.171		0.009
H14-	PHVU -> PHS	1.137	-0.172	(-0.313, -0.038)	0.018	**	0.027
H15-	PHSE -> PHS	1.137	-0.018	(-0.134, 0.167)	0.811		0.000
H16+	PPR*PHS -> ITD	1.305	-0.116	(-0.246, 0.037)	0.116		0.014
H17-	HMO*PHS -> ITD	2.069	-0.155	(-0.314, -0.010)	0.048	**	0.021
H18-	PEX*PHS -> ITD	2.054	0.059	(-0.094, 0.208)	0.438		0.003
H19-	PHS -> ITA	1.063	0.000	(-0.108, 0.111)	0.993		0.000
H20+	ITD -> ITA	1.259	0.296	(0.137, 0.458)	0.000	***	0.113

7 Discussion

Our research model emphasizes the multi-dimensional role that privacy plays in regards to whether users accept healthcare-related wearable devices. To develop our model, we adapted well-established theories in the technology acceptance and privacy domain. Our results afford noteworthy evidence that privacy truly poses a serious concern for potential users and that, when joined with benefits to disclosure, an individual's perceived health status moderates it. Specific to the research questions guiding this research endeavor, we found significant evidence in regards to the impact that the privacy calculus has on intentions to disclose information on the decision process to adopt healthcare wearables (RQ1). In addition, we observed evidence of the privacy paradox in the context of healthcare wearables acceptance (RQ2). The following narrative explains our findings.

PTV had a somewhat inconclusive effect on PPR with the p-value 0.135; however, PTS had the highest significant positive effect, REF had a significant negative effect, and SEF had a somewhat negative effect on PPR. We may ascribe the inconclusiveness effect that PTV had on PPR to insufficient knowledge among survey participants in regards to threats to privacy specific to wearables, an emerging health technology (Sun et al., 2013). Even so, that we found support for H2 through H4 supports the reality of the risk calculus where balancing threats with the ability to cope determines one's concerns about privacy (Zhang et al., 2018). PPR had a significant negative effect on ITD, which means that threats to one's privacy and the ability to respond impacts one's concern with privacy and one's inclination to disclose personal information.

We found HMO to have a somewhat significant positive effect on ITD. We also found it to have a significant positive effect on ITA. However, we found PEX to have the greatest significant positive effect on both ITD and ITA. Accordingly, we understand that the pleasure of using a wearable device and the expectation that the device will deliver the expected benefit inspires one to disclose one's private information and accept wearables.

In reference to RQ1, our findings that support H5, H6, and H8 offers evidence of the privacy calculus, which conceptualizes the privacy trade-off process where users evaluate privacy risks in light of the benefits associated with disclosure (Kehr et al., 2015). These results align with other health/privacy-oriented research (Zhang et al., 2018). In addition, the net confirmation of H2 through H8 provides support regarding the dual-calculus model, which contemplates both the risk calculus and the privacy calculus in the disclosure decision process (Li, 2012).

Among the four constructs EEX, SIN, TSE, and FCG, only SIN had a somewhat significant positive impact on ITA. Accordingly, we did not find support for H10, H12, and H13 but found partial support for H11. We can conclude that the effort required, a person's confidence in their ability to use the device, and the perceived suitability to satisfy expectations have no significant effect on adopting a wearable device; however, other people somewhat influences wearable adoption but only at minimal levels. This finding corresponds to past wearable research, such as Patton (2018), that has also discovered inconclusive evidence about similar constructs to ITA. We may explain these results based on the fact that our sample contained an evenly distributed age range between 24 and 64 (see Table 2 above), which could also explain the decreased levels of normality that we discovered for the noted constructs. Research has shown age to significantly affect factors related to technology acceptance (Morris & Venkatesh, 2000; Venkatesh et al., 2012) and to potentially skew results when corporately examined.

Another possible reason for why EEX, TSE, and FCG did not perform well concerns the category of the wearable device (whether one uses it for a specific medical condition or for general fitness). In our study, 96 percent of the survey participants reported being in fair to excellent health, 88 percent reported that a physician had neither recommended nor mandated them to use a device, and 77 percent had no chronic condition, which signifies a fairly healthy pool of respondents. Thus, overall, we conclude that study participants mostly focused on using fitness-oriented devices in our survey. Prior research (Gao et al., 2015) has identified fitness wearable device users as more anxious about privacy and about the value others place on using a wearable device. Research has also found age to be an extenuating factor (Gao et al., 2015), possibly because an older population generally has more health concerns and might be more likely to pursue a healthcare-oriented wearable device to address a specific medical issue. Accordingly, we recognize that the type of device considered and/or a participant's age might also explain why EEX, TSE, and FCG performed poorly and why SIN performed somewhat better.

We found PHVU to have a significant negative influence on PHS, which confirms H14; however, PHSE did not have a significant negative influence on PHS, which does not support H15. We conclude that vulnerability to health issues does negatively affect one's perceived health status. H16, H17, and H18 focus on the moderating influence that individuals' perceived health status has on their intention to disclose private information. We found that a higher PHS had a somewhat significant positive effect on the influence that PPR had on ITD at a significance level just above 0.10, which means that upsurges in how one perceives one's health increases the effect that their privacy risk perceptions have on one's intention to disclose private information, which somewhat affirms H16. Regarding healthcare wearables, people care more about the cost or risks associated with disclosing their private information when they have a higher perceived health status (i.e., perceive themselves as healthier). We also found that a higher PHS had a significant negative impact on the influence that HMO had on ITD, which confirms H17. People place less importance on pleasure when they have a higher perceived health status. Finally, we perceived that PHS had no significant impact on PEX, which does not support H18. We can conclude that, with a higher PHS, people's concern for privacy has a higher negative influence on their intention to disclose, while the expected enjoyment they expect to receive from using a healthcare-related wearable device only has a small positive influence on their decision to disclose their personal information. In reference to RQ2, we found perception of one's health status does moderate the disclosure decision process, which confirms that the privacy paradox exists.

We found that PHS had no significant influence on ITA, which does not support H19. However, we did find that ITD had a significant positive effect on ITA, which supports H20. We can conclude that people's intentions to disclose private information does affect whether or not they intend to adopt a wearable device. This conclusion aligns with Gao et al. (2015) who found that the single construct privacy significantly contributed to explaining wearable acceptance. In our study, we extended the privacy construct in order to capture the complex behavioral progressions surrounding its presence, which we conceptualized via the risk calculus, the privacy calculus, and the privacy paradox. Not only did the results correlate with Gao et al's (2015), but we also perceived a greater influence in that ITD explained 29.6 percent of the variance of ITA in our study compared to the 21.5 percent that the singular privacy constructed account for in Gao et al. (2015).

8 Conclusion

The process to accept healthcare wearable devices features numerous influences and thought processes, which we can partially attribute to the sensitive information that these devices capture. While past research has fixated on specific privacy and acceptance aspects (Gao et al., 2015; Harmon, 2019; Scott, 2020), a gap remained in that we lacked work that comprehensively examined privacy in the healthcare-related wearable domain. Based on recognized research in the technology acceptance area, PMT, HBM, and privacy calculus theories, we contribute to filling that gap in this study by conceptualizing these influences and thought processes into a research model that we could measure and evaluate with a representative sample of the populace. In particular, we focused on examining privacy in the form of the privacy calculus (RQ1) and the privacy paradox (RQ2) in the wearable device acceptance domain. Using survey research and PLS-SEM analyses, we found evidence for both theories in wearable acceptance.

Our study meaningfully expands what we presently know about the healthcare wearables' privacy/acceptance paradigm. In particular, we expand previous efforts (e.g., Gao et al., 2015; Li et al., 2016; Zhang et al., 2018) that have focused on specific research domains of the wearables paradigm and/or health privacy by combining antecedents to privacy disclosure with antecedents to technology acceptance.

Additionally, we introduced the construct perceived health status to capture how people feel about their health and how that perception contributes to whether they accept technology. Accordingly, this study helps more holistically explain the decision processes intrinsic to using an emerging technology, such as wearables, that has seemingly proven itself to add significance and practical value to those who use it.

Wearable devices no longer constitute a fad that people use for curiosity's sake; indeed, some sources expect wearables sales to reach US$189.9 million in 2022 (Ubrani et al., 2018). Consumers continue to discover genuine value in their use, especially in the health-related wearables domain, which offers increased management and support of one's health and wellbeing. However, using wearable devices comes with some (particularly privacy-related) risks. Researchers, manufactures, and healthcare organizations must comprehend the role that the risk calculus, the privacy calculus, and the privacy paradox play in regards to the decision-making process that consumers go through to decide whether to disclose or not to disclose personal information. The issue becomes particularly pronounced with healthcare wearable devices due to their potential negative impact on individuals' health and wellbeing (should they opt to avoid the technology) and the risk the devices pose to individuals' privacy (should they opt to accept it). By recognizing privacy's importance to consumers, manufacturers, in concert with healthcare professionals, can emphasize security in designing and implementing wearables and, thus, increase user confidence in whether wearable devices protect their personal information.

For researchers, our findings add to our knowledge about the role that the privacy calculus theories play in the acceptance of healthcare-related wearables. This increased knowledge will enhance future research endeavors in the same space, especially in the realm of the privacy paradox, which a cloak of obscurity continues to surround (Gerber et al., 2018; Kokolakis, 2017). For wearable manufacturers, designing security-oriented devices will raise user confidence and help ensure that people use them (Shim et al., 2020). For healthcare organizations, who continue to increase deployment of wearables as a part of patient care, understanding and addressing privacy concerns and barriers to disclosure and acceptance will increase confidence in wearables and thus utilization by their patients. Understanding also highlights the importance of transparency and ethics in regards to what information is captured and what parties will have access to it. This study further informs privacy and the healthcare-related wearable space, enhancing the value proposition of this recent and promising area of technology.

Of course, as with any study, ours has several limitations. First, we examined healthcare wearable devices in general without consideration as to how different types of wearable devices might influence the privacy/disclosure decision process. Second, we did not consider specific health concerns; rather, we only considered users' general health status. Third, no respondent in our sample reported very poor health. Accordingly, our study does not adequately consider the full health-status spectrum. Fourth, we found a similar inadequacy for education given that our sample lacked respondents without a degree.

Our work opens up several opportunities for future research. First, researchers could resample the population and perform a similar analysis with the intent to address this study's deficiencies in regards to health status, device type, and education. Health status and device type would be particularly useful in order to shed light on our hypotheses that lacked support. Second, we perceive an opportunity related to categorical moderation analysis (PLS-MGA) (Wong, 2019) based on participant demographics such as usage, chronic health condition, age, and education. A focus on participant demographics would offer a significant opportunity to compare the moderating effect in the context of each category. Lastly, researchers have an opportunity to adjust our research model (based on our findings) and focus on specific types of wearables in order to analyze and further understand the role of the privacy calculus and privacy paradox in the context of specific types of wearables.

References

Anaya, S. L. H., Alsadoon, A., Costadopoulos, N., & Prasad, P. W. C. (2018). Ethical implications of user perceptions of wearable devices. *Science Engineering Ethics*, *24*, 1-28.

Barth, S., & de Jong, M. D. T. (2017). The privacy paradox—investigating discrepancies between expressed privacy concerns and actual online behavior—a systematic literature review. *Telematics and Informatics*, *34*(7), 1038-1058.

Bélanger, F., & Crossler, R. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, *35*(4), 1017-1041.

Brown, S. (2005). Model of adoption of technology in households: A baseline model test and extension incorporating household life cycle. *MIS Quarterly*, *29*(3), 399-426.

Clarke, R. (1999). Internet privacy concerns confirm the case for intervention. *Communications of the ACM*, *42*(2), 60-67.

Davis, F., Bagozzi, R., & Warshaw, P. (1989). User acceptance of computer technology: A comparison of two. *Management Science*, *35*(8), 982-1003.

Davis, F. D. (1986). *A technology acceptance model for empirically testing new end-user information systems: Theory and results* (unpublished doctoral dissertation). Massachusetts Institute of Technology.

Deng, Z., & Liu, S. (2017). Understanding consumer health information-seeking behavior from the perspective of the risk perception attitude framework and social support in mobile social media websites. *International Journal of Medical Informatics*, *105*, 98-109.

Dittrich, R., Francis, B., Hatzinger, R., & Katzenbeisser, W. (2007). A paired comparison approach for the analysis of sets of Likert-scale responses. *Statistical Modelling*, *7*(1), 3-28.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*. Addison-Wesley.

GAO. (2017). *Internet of things: Status and implications of an increasingly connected world*. Retrieved from https://www.gao.gov/assets/690/684590.pdf

Gao, Y., He, L., & Luo, Y. (2015). An empirical study of wearable technology acceptance in healthcare. *Industrial Management & Data Systems*, *115*(9), 1704-1723.

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, *77*, 226-261.

Hae-Young, K. (2013). Statistical notes for clinical researchers: Assessing normal distribution (2) using skewness and kurtosis. *Restorative Dentistry & Endodontics*, *38*(1), 52-54.

Hair, J. F., Hult, G. T. M., Gingle, C. M., & Sarstedt, M. (2017). *A primer on partial least squares structural equation modeling (PLS-SEM)* (2nd ed.). Sage.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice*, *19*(2), 139-152.

Hair, J. F. J., Ringle, C. M., & Sarstedt, M. (2013). Partial least squares structural equation modeling: Rigorous applications, better results and higher acceptance. *Long Range Planning*, *46*(1-2), 1-12.

Hair, J. J. F., Howard, M. C., & Nitzl, C. (2020). Assessing measurement model quality in PLS-SEM using confirmatory composite analysis. *Journal of Business Research*, *109*, 101-110.

Harmon, A. (2019). *A quantitative predictive study of U.S. Fitbit owners' intentions to use activity trackers* (doctoral dissertation). Capella University.

Harper, A. (2016). *The impact of consumer security awareness on adopting the Internet of things: A correlational study* (doctoral dissertation). Capella University.

Hassija, V., Chamola, V., Bajpai, B. C., Naren, & Zeadally, S. (2021). Security issues in implantable medical devices: Fact or fiction? *Sustainable Cities and Society*, 66.

Huber, F., Vollhardt, K., Matthes, I., & Vogel, J. (2010). Brand misconduct: Consequences on consumer–brand relationships. *Journal of Business Research*, *63*(11), 1113-1120.

Janz, N. K., & Becker, M. H. (1984). The health belief model: A decade later. *Health Education*, *11*(1), 1-47.

Jayden, K. (2018). Tapping into the wearable device revolution in the work environment: A systematic review. *Information Technology & People*, *31*(3), 791-818.

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, *25*(6), 607-635.

Kenny, D. A. (2018). *Moderation*. Retrieved from http://davidakenny.net/cm/moderation.htm

Kim, J. A., Yang, S. J., Chee, Y. K., Kwon, K. J., & An, J. (2015). Effects of health status and health behaviors on depression among married female immigrants in South Korea. *Asian Nursing Research*, *9*(2), 125-131.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122-134.

Kritzler, M., Tenfält, A., Bäckman, M., & Michahelles, F. (2015). Wearable technology as a solution for workplace safety. In *Proceedings of the 14th International Conference on Mobile and Ubiquitous Multimedia.*

Lehto, M., & Lehto, M. (2017). Health information privacy of activity trackers. In *Proceedings of the 16th European Conference on Cyber Warfare and Security.*

Li, H., Wu, J., Gao, Y., & Shi, Y. (2016). Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective. *International Journal of Medical Informatics*, *88*, 8-17.

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems*, *54*(1), 471-482.

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

Privacy. (2017). In *Merriam-Webster*. Retrieved from https://www.merriam-webster.com/dictionary

Meyer, J., Fortmann, J., Wasmann, M., & Heuten, W. (2015). Making lifelogging usable: Design guidelines for activity trackers. In *Proceedings of the International Conference on MultiMedia Modeling.*

Morris, M. G., & Venkatesh, V. (2000). Age differences in technology adoption decisions: Implications for a changing work force. *Personnel Psychology*, *53*(2), 375-403.

Muaremi, A., Arnrich, B., & Tröster, G. (2013). Towards measuring stress with smartphones and wearable devices during workday and sleep. *BioNanoScience*, *3*(2), 172-183.

Nadeem, A., Hussain, M. A., Owais, O., Salam, A., Iqbal, S., & Ahsan, K. (2015). Application specific study, analysis and classification of body area wireless sensor network applications. *Computer Networks*, *83*, 363-380.

Norberg, P., Horne, D., & Horne, D. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *The Journal of Consumer Affairs*, *41*(1), 100-126.

Padyab, A., & Ståhlbröst, A. (2018). Exploring the dimensions of individual privacy concerns in relation to the Internet of things use situations. *Digital Policy, Regulation and Governance*, *20*(6), 528-544.

Patton, W. (2018). *Application of UTAUT2 to the adoption of smartwatch technology by American consumers* (Doctoral dissertation). Capella University.

Perez, A. J., & Zeadally, S. (2018). Privacy issues and solutions for consumer wearables. *IT Professional*, *20*(4), 46-56.

Preusse, K. C., Mitzner, T. L., Fausset, C. B., & Rogers, W. A. (2017). Older adults' acceptance of activity trackers. *Journal of Applied Gerontology*, *36*(2), 127-155.

Pulipaka, S. (2019). *Impact of privacy concerns and user perceptions on the usage intention of wearable smart medical devices: A correlational study* (doctoral dissertation). Capella University.

Rainie, L., Kiesler, S., Kang, R., Madden, M., Duggan, M., Brown, S., & Dabbish, L. (2013). Anonymity, privacy, and security online. *Pew Research Center.* Retrieved from https://www.pewresearch.org/internet/2013/09/05/anonymity-privacy-and-security-online/

Ringle, C. M., Wende, S., & Becker, J.-M. (2015). *SmartPLS 3*. Retrieved from http://www.smartpls.com

Roberts, T. (2012). Understanding survey research: Applications and processes. *British Journal of Midwifery*, *20*(2), 114-120.

Romano, N. C., Jr., & Fjermestad, J. (2007). Privacy and security in the age of electronic customer relationship management. *International Journal of Information Security and Privacy, 1*(1), 65-86.

Scott, D. (2020). *A correlation study of smartwatch adoption and privacy concerns with U.S. consumers using the UTAUT2* (doctoral dissertation). Colorado Technical University.

Shen, N. (2019). *The eHealth trust model: Understanding the patient privacy perspective in a digital health environment* (doctoral dissertation). University of Toronto.

Shim, J., Sharda, R., French, A. M., Syler, R. A., & Patten, K. P. (2020). The Internet of things: Multi-faceted research perspectives. *Communications of the Association for Information Systems*, *46*, 511-536.

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

Spiekermann, S., Grossklags, J., & Berendt, B. (2001). E-privacy in 2nd generation e-commerce: Privacy preferences versus actual behavior. In *Proceedings of the 3rd ACM Conference on Electronic Commerce*.

Straub, D., Boudreau, M.-C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Association for Information Systems*, *13*, 380-427.

Sun, Y., Wang, N., Guo, X., & Peng, Z. (2013). Understanding the acceptance of mobile health services: A comparison and Iintegration of alternative models. *Journal of Electronic Commerce Research*, *14*(2), 183-200.

Turow, J., Hennessy, M., & Draper, N. (2015). The tradeoff fallacy: How marketers are misrepresenting american consumers and opening them up to exploitation. *SSRN*. Retrieved from https://ssrn.com/abstract=2820060

Ubrani, J., Llamas, R., & Shirer, M. (2018). IDC forecasts sustained double-digit growth for wearable devices led by steady adoption of smartwatches. *Business Wire*. Retrieved from https://www.businesswire.com/news/home/20181217005099/en/idc-forecasts-sustained-double-digit-growth-wearable-devices

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, *46*(2), 186-204.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*(3), 425-478.

Venkatesh, V., Thong, J., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly*, *36*(1), 157.

Vitak, J., Liao, Y., Kumar, A., Zimmer, M., & Kritikos, K. (2018). Privacy attitudes and data valuation among fitness tracker users. In G. Chowdhury, J. McLeod, V. Gillet, & P. Willett (Eds.), *Transforming digital worlds* (LNCS vol. 10766). Springer.

Wei, Z., & Piramuthu, S. (2014). Security/privacy of wearable fitness tracking IoT devices. In *Proceedings of the 9th Iberian Conference on Information Systems and Technologies*.

Wenling, W., Rajneesh, S., & Shan, F. (2015). The role of product personalization in effects of self-congruity versus functional congruity. *Journal of Travel Research*, *38*, 340-352.

Williams, M., Nurse, J. R. C., & Creese, S. (2016). The perfect storm: The privacy paradox and the Internet-of-things. In *Proceedings of the 11th International Conference on Availability, Reliability and Security*,

Wilson, D. W., & Valacich, J. S. (2012). Unpacking the privacy paradox: Irrational decision-making within the privacy calculus. In *Proceedings of the 33rd International Conference on Information Systems*.

Wong, K. K.-K. (2019). *Mastering partial least squares structural equation modeling (PLS-SEM) with SmartPLS in 38 hours*. iUniverse.

Wong, K. K. (2013). Partial least squares structural equation modeling (PLS-SEM) techniques using SmartPLS. *Marketing Bulletin*, *24*, 1-32.

Woon, I., Tan, G., & Low, R. (2005). A protection motivation theory approach to home wireless security. In *Proceedings of the 26th International Conference on Information Systems.*

Yang, K., Ahn, C. R., Vuran, M. C., & Aria, S. S. (2016). Semi-supervised near-miss fall detection for ironworkers with a wearable inertial measurement unit. *Automation in Construction*, *68*, 194-202.

Zenonos, A., Khan, A., Kalogridis, G., Vatsikas, S., Lewis, T., & Sooriyabandara, M. (2016). HealthyOffice: Mood recognition at work using smartphones and wearable sensors. In *Proceedings of the 2nd IEEE International Workshop on Sensing Systems and Applications Using Wrist Worn Smart Devices.*

Zhang, X., Liu, S., Chen, X., Wang, L., Gao, B., & Zhu, Q. (2018). Health information privacy concerns, antecedents, and information disclosure intention in online health communities. *Information & Management*, *55*(4), 482-493.

Zhou, W., Jia, Y., Peng, A., Zhang, Y., & Liu, P. (2019). The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. *IEEE Internet of Things Journal*, *6*(2), 1606-1616.

Appendix A: Research Model Constructs Measurements

Seven-point Likert scale

Perceived threat vulnerability (PTV) (Zhang et al., 2018)

PTV1. My information privacy is at risk of being invaded.

PTV2. It is likely that my information privacy will be invaded.

PTV3. It is possible that my information privacy will be invaded.

PTV4. My information privacy is not safe from being invaded.

Perceived threat severity (PTS) (Zhang et al., 2018)

PTS1. If my information privacy is invaded, it would be severe.

PTS2. If my information privacy is invaded, it would be serious.

PTS3. If my information privacy is invaded, it would be significant.

PTS4. If my information privacy is invaded, it would not be irrelevant.

Response efficacy (REF) (Zhang et al., 2018)

REF1. The privacy protection measures provided by healthcare wearable manufacturers are suitable for protecting my personal information.

REF2. The privacy protection measures provided by healthcare wearable manufacturers can effectively protect my personal information.

REF3. My personal information is more likely to be protected when using privacy protection measures provided by healthcare wearable manufacturers.

Task self-efficacy (SEF) (Zhang et al., 2018)

SEF1. Protecting my information privacy is easy for me when using healthcare wearable devices.

SEF2. I have the capability to protect my information privacy when using healthcare wearable devices.

SEF3. I am able to protect my information privacy without much effort when using healthcare wearable devices.

SEF4. Protecting my information privacy is not difficult when using healthcare wearable devices.

Perceived privacy risk (PPR) (Zhang et al., 2018)

PPR1. I believe that submitting health and other privacy information for the purpose of using wearable devices is not advisable at all.

PPR2. Health and other privacy information submitted for the purpose of using wearable devices will be abused for sure once submitted.

PPR3. Health and other privacy information submitted for the purpose of using wearable devices could be shared or sold to others once submitted.

Hedonic motivation (HMO) (Gao et al., 2015)

HMO1. Healthcare wearable devices are fun to use.

HMO2. Healthcare wearable devices are enjoyable to use.

HMO3. Healthcare wearable devices are entertaining to use.

HMO4. Healthcare wearable devices are not boring to use.

Performance expectancy (PEX) (Gao et al., 2015)

PEX1. Healthcare wearable devices add value to my personal life.

PEX2. Using healthcare wearable devices helps me to achieve my healthcare goals more quickly.

PEX3. Using healthcare wearable devices enhances the quality of my daily healthcare requirements.

Effort expectancy (EEX) (Gao et al., 2015)

EEX1. It is easy for me to learn how to use healthcare wearable devices.

EEX2. Healthcare wearable devices are easy to use.

EEX3. Becoming skillful at using healthcare wearable devices is easy for me.

EEX4. Healthcare wearable device are not difficult to use.

Social influence (SIN) (Gao et al., 2015)

SIN1. Others who are important to me would feel that I should use a healthcare wearable device.

SIN2. Others who influence me would feel that I should use a healthcare wearable device.

SIN3. Others whose opinions I value would prefer that I should use a healthcare wearable device.

Technology self-efficacy (TSE) (Gao et al., 2015)

TSE1. Using wearable devices make it easy for me to self-monitor my health-related conditions.

TSE2. I am capable to use healthcare wearable devices to self-monitor my health-related conditions.

TSE3. It takes little effort to use healthcare wearable devices to self-monitor my health-related conditions.

Functional congruence (FCG) (Gao et al., 2015)

FCG1. Healthcare wearable devices are anticipated to be comfortable to use.

FCG2. Healthcare wearable devices are anticipated to be fashionable.

FCG3. Healthcare wearable devices are anticipated to be priced appropriately according to device quality.

FCG4. Healthcare wearable devices are not anticipated to be unpleasant to use.

Perceived health vulnerability (PHVU) (Gao et al., 2015)

PHVU1. I am at risk of suffering one or more of the following concerns: having little knowledge about self-healthcare, monitoring personal daily healthcare, and/or suffering health-related diseases.

PHVU2. It is likely that I will suffer one or more of the following concerns: having little knowledge about self-healthcare, monitoring personal daily healthcare, and/or suffering health-related diseases.

PHVU3. It is possible for me to suffer one or more of the following concerns: having little knowledge about self-healthcare, monitoring personal daily healthcare, and/or suffering health-related diseases.

Perceived health severity (PHSE) (Gao et al., 2015)

PHSE1. It would be severe if I suffered one or more of the following concerns: having little knowledge about self-healthcare, monitoring personal daily healthcare, and/or suffering health-related diseases.

PHSE2. It would be serious if I suffered one or more of the following concerns: having little knowledge about self-healthcare, monitoring personal daily healthcare, and/or suffering health-related diseases.

PHSE3. It would be significant if I suffered one or more of the following problems: having little knowledge about self-healthcare, monitoring personal daily healthcare, and/or suffering health-related diseases.

Intention to disclose (ITD) (Zhang et al., 2018)

ITD1. I am likely to provide general personal information in the use of healthcare wearable devices (e.g., such as name, email, profile image, etc.).

ITD2. I am likely to provide specific personal information in the use of healthcare wearable devices (e.g., such as DOB, gender, ethnicity, race, etc.).

ITD3. I am likely to provide personal fitness and health information in the use of healthcare wearable devices (e.g., such as fitness activity, exercise routines, medications, health history, vital signs, etc.).

Intention to adopt healthcare wearable devices (ITA) (Gao et al., 2015)

ITA1. I anticipate using a healthcare wearable device in the future.

ITA2. I have plans to use a healthcare wearable device whenever possible.

ITA3. I foresee increasing use of healthcare wearable devices in the future.

ITA4. I do not anticipate avoiding the use of healthcare wearable devices in the future.

Interval scale measurements

Perceived health status (PHS) (Kim et al., 2015)

1) Very poor
2) Poor
3) Fair
4) Good
5) Excellent

Demographic

Use recommended, mandated, or neither (USE)

1) Recommended
2) Mandated
3) Neither

Current chronic health condition (CHC)

1) Yes
2) No

Gender (GDR)

1) Male
2) Female

Age (AGE) (Malhotra et al., 2004).

1) 24 or under
2) 25-34
3) 35-44
4) 45-54
5) 55-64
6) 65 or older

Highest level of education completed (EDU) (Malhotra et al., 2004)

1) Some school, no degree
2) High school graduate
3) Some college, no degree
4) Bachelor’s degree
5) Master’s degree
6) Professional degree
7) Doctoral degree

About the Authors

Thomas Jernejcic is a Professor of Computer Information Technology at California Baptist University (CBU). He received his BA in Business Administration from CBU and MS and PhD degrees in Information Systems (IS) from Dakota State University (DSU) with specializations in Data Management and Information Assurance and Computer Security. He has served as Program Coordinator for various IS BS degrees as well as Director of the MS in Information Technology Management program and Director of Online Education at CBU, Jabs School of Business. His 34 years of IS industry experience includes various roles such as programmer analyst, software engineer, systems programmer, system administrator, and database administrator as well as supervising and managing others in similar roles. His primary research interests include privacy, information assurance, cybersecurity, cloud computing, big data, and gamification. He has participated as peer reviewer on multiple publications. He is a member of the Association for Information Systems (AIS).

Omar El-Gayar is a Professor of Information Systems at Dakota State University. He has an extensive administrative experience at the college and university levels as the Dean for the College of Information Technology, United Arab Emirates University (UAEU) and the Founding Dean of Graduate Studies and Research, Dakota State University. His research interests include: analytics, business intelligence, and decision support with applications in problem domain areas such as healthcare, environmental management, and security planning and management. His inter-disciplinary educational background and training is in information technology, computer science, economics, and operations research. His industry experience includes working as an analyst, modeler, and programmer. His numerous publications appear in various information technology related fields. He serves as a peer and program evaluator for accrediting agencies such as the Higher Learning Commission and ABET, as a panelist for the National Science Foundation, and as a peer reviewer for numerous journals and conferences. He is a member of a number of professional organizations such as the Association for Information Systems (AIS) and the Association for Computing Machinery (ACM).

Transactions on Human – Computer Interaction