Klossner, Sara; Ghanbari, Hadi; Rossi, Matti; Sarv, Lill

Personalization-Privacy Paradox in Using Mobile Health Services

Published in:
ECIS 2023 Proceedings

Published: 11/05/2023

Document Version
Publisher's PDF, also known as Version of record

Please cite the original version:
Klossner, S., Ghanbari, H., Rossi, M., & Sarv, L. (2023). Personalization-Privacy Paradox in Using Mobile Health Services. In *ECIS 2023 Proceedings* Article 346 (European Conference on Information Systems). Association for Information Systems. https://aisel.aisnet.org/ecis2023_rp/346/

5-11-2023

Personalization-Privacy Paradox in Using Mobile Health Services

Sara Klossner
Aalto University School of Business, sara.klossner@aalto.fi

Hadi Ghanbari
Aalto University School of Business, hadi.ghanbari@aalto.fi

Matti Rossi
Aalto University School of Business, matti.rossi@aalto.fi

Lill Sarv
Tallinn University of Technology, lill.sarv@taltech.ee

PERSONALIZATION-PRIVACY PARADOX IN USING MOBILE HEALTH SERVICES

Research Paper

Sara, Klossner, Aalto University School of Business, Finland, sara.klossner@aalto.fi

Hadi, Ghanbari, Aalto University School of Business, Finland and FinEst Centre for Smart Cities, Estonia, hadi.ghanbari@aalto.fi

Matti, Rossi, Aalto University School of Business, Finland, matti.rossi@aalto.fi

Lill, Sarv, Tallinn University of Technology, Estonia, lill.sarv@taltech.ee

Abstract

The rapid growth of the population and the increase in life expectancy put intense pressure on the healthcare systems worldwide. Mobile health applications (m-health apps) can help ease the situation by offering highly personalized services that empower individuals to take better care of their health. To reach their full potential, m-health apps must continuously gather personal health data from users, which leads to privacy concerns. We study the influence of users' privacy concerns on their intention to disclose personal health data to m-health apps. Using an online survey and conducting SEM-PLS, we show that a personalization-privacy paradox is present in the context of m-health apps. While respondents claim to have privacy concerns about using m-health apps, their concerns do not negatively affect their self-disclosure intentions nor their intention to continue using the apps. Our results show that the magnitude of personalization-privacy paradox is influenced by demographic factors.

Keywords: Mobile health, Privacy, Artificial Intelligence, Femtech, Healthcare.

1 Introduction

With the growing population and urbanization, health concerns arise in modern societies. Nowadays, five out of the top ten causes of death globally are related to unhealthy behavior (Deloitte, 2021). In addition to the unhealthy lifestyles of citizens, the population is aging in welfare countries (Deloitte, 2021). The simultaneous increase in the life expectancy and increase in the need for chronic care is leading to a doctor shortage worldwide (Meskó et al., 2018). Thus, the capacity constraints of the healthcare sector make it impossible to meet the growing demand for one-to-one appointments between patients and doctors or therapists. Especially the COVID-19 pandemic has highlighted the capacity constraints of healthcare systems all over the world and the need for preventive solutions to improve citizens' health at scale. To that end, smart mobile health applications (m-health apps) play an important role in preventing diseases and also in diagnosis and rehabilitation (Cook et al., 2018, Zhao et al., 2018).

Citizens can benefit from various m-health apps, ranging from wearable technologies to femtech and digital therapy apps. These apps use Artificial Intelligence (AI) to process users' vitals and health records to provide them with personalized recommendations. Considering that AI enables faster and more accurate decision-making and diagnosis (Jiang et al., 2017), m-health apps can help treat patients at scale, providing them with low-cost, high-quality, and around-the-clock access to healthcare services (Kao and Liebovitz, 2017, Zhou et al., 2019). M-health apps are specifically beneficial for providing personalized services to citizens (Zhao et al., 2018), empowering them to actively engage in their

healthcare and well-being. However, to provide such optimal and highly personalized services, m-health apps are dependent on the self-disclosure of sensitive personal information by users. Considering that leaking this sensitive health data can have detrimental consequences for patients and companies, privacy concerns increase simultaneously with the level of personalization offered by m-health apps (Guo et al., 2016). Still, previous research shows that many m-health apps violate users' privacy (Papageorgiou et al., 2018). For instance, Flo, one of the most popular period tracking apps, shared the extremely sensitive and intimate data of its users with Google and Facebook in 2019 (Gupta and A., 2021).

Past research shows that often there is a paradox between people's privacy concerns and their interest in highly personalized digital services (Guo et al., 2016, Liu and Tao, 2022). Users often claim to be concerned about data privacy (Gerber et al., 2018, Zhou et al., 2019, Lidynia et al., 2019) but act in a controversial way (Gerber et al., 2018), for example, by disclosing too much personal information about themselves. Previous studies claim that users often decide to disclose or retain information to a digital service by assessing the potential benefits and risks that the information sharing might bring (Krasnova et al., 2012, Zhang et al., 2018). To that end, in addition to privacy concerns and the level of personalization, users' trust in a service, level of technological self-efficacy, and demographic factors such as age and education have shown to play an influential role (Zhang et al., 2018, Kang and Jung, 2021, Liu and Tao, 2022, Krasnova et al., 2012, Zhou et al., 2019). However, to the best of our knowledge, little is known about the interrelationship between these factors and how they affect the personalization-privacy paradox in using m-health apps. Therefore, to gain a better understanding of the privacy concerns of citizens about m-health apps and how such concerns affect their intention to use and share personal health information with these apps, we set out to answer the following question: ***How do users' privacy concerns affect their self-disclosure intention while using m-health apps?***

To answer this question, we developed a theoretical model drawing on well-established Information Systems (IS) theories and concepts on information privacy. To test the theoretical model, we collected data via an online survey (n=249) and conducted a PLS-SEM analysis using SPSS AMOS software. Our results show that while the respondents claim to have privacy concerns about using m-health apps, these concerns do not have a negative effect on their self-disclosure intentions. Additionally, the level of personalization increased females' privacy concerns significantly, but the influence was not significant for men. At the same time, privacy concerns had a significant negative effect on self-disclosure in the male group. Self-efficacy was found to have a significant impact on decreasing privacy concerns and increasing self-disclosure. Privacy concerns, in turn, were found to have a significant negative effect on trust, while trust had a significant positive effect on users' self-disclosure intention.

Our study makes several contributions to IS research and practice by providing a more nuanced understanding of personalization-privacy paradox in the m-health context. We specially shed light on how differences in age, gender, educational level, and level of digital skills impact the personalization-privacy paradox. Our study provides companies with insights on tackling users' privacy concerns. This, in turn, could enable broader adoption of m-health apps and unlock their benefits for society at large.

2 Research Background

2.1 M-health apps

The World Health Organization (WHO, 2019) states that digital health encompasses the themes of electronic health, AI, the internet of things, and computational methods applied to big data and genomics. Thus, the citizens' health journey will be more and more interlinked with data, analytics, and AI not only during and after treatment but also in a preventive manner.

M-health apps can encourage citizens toward a more active lifestyle, as especially diseases triggered by unhealthy lifestyles are a growing problem for the healthcare sector. These apps can motivate users to exercise more, eat better, take more responsibility for their own health and help them also listen to their bodies and learn when it is time to rest (Härkönen and Räsänen, 2021). In addition, with the help of these apps, users can measure bodily functions, which was previously possible only with the support of

health professionals (Koivumäki et al., 2017). M-health apps can recognize patterns from these health data to predict both physical and mental diseases such as diabetes and depression in their early stages (Cook et al., 2018). This, in turn, enables users to better manage their personal health and prevent diseases (Kukafka, 2019). M-health apps also enable healthcare providers to innovate solutions for disease prevention plans and treatment for chronic diseases (Kotz et al., 2016).

Kao and Liebovitz (2017) categorize m-health apps into six categories: wellness management, disease management, self-diagnosis, medication reminders, electronic patient portals, and physical medicine and rehabilitation. In this paper, we concentrate on the category of wellness apps that individuals use based on their own motivation. The wellness apps aim to encourage consumers to engage in a healthier lifestyle, for example, by tracking their sleep, exercise, and diet. There is a wide range of m-health apps including, for example, smartwatches and rings, fitness apps, mindfulness, and mental health apps. The wellness category also comprises femtech applications which provide digital healthcare solutions for women, including maternal and menstrual health. We also consider mental wellness apps as a part of the wellness management category. In the mental health space, there are various apps from general mindfulness and meditation apps to apps connecting users to a real therapist remotely.

Most m-health apps rely on AI to provide users with personalized services. AI has been changing the field of healthcare, as the availability of healthcare data is increasing, and analytics techniques are developing (Jiang et al., 2017). One of the greatest advantages of AI is that it can manage and interpret information much more effectively than humans have the cognitive capacity to. As such, AI is accelerating the change in healthcare from a generalized approach to a highly personalized, preventive, and participatory approaches, where the main focus is on individuals and data (Koivumäki et al., 2017). Thus, by providing personalized services to a large number of citizens, AI can help improve disease prevention and rehabilitation and ultimately reduce healthcare costs (Matheny, 2019, Cook et al., 2018). However, to provide such valuable services, AI-enabled m-health services need to collect more and more sensitive health information from users. This creates privacy concerns for citizens and obligations for healthcare providers and the companies who collect the data. Information privacy and security are found to be amongst the main concerns and barriers to incorporating technology into healthcare (Cook et al., 2018), as they might hinder citizens' acceptance of digital health technologies (Becker, 2018).

2.2 Privacy in healthcare

Tracking and analyzing user data creates benefits for users through personalized services but simultaneously poses a privacy risk. And the more personalized the service is, the higher the privacy risk tends to be. Privacy risks related to personalized services can include, for example, surveillance by government agencies and private companies and information theft (Kotz et al., 2016). Therefore, there must be legitimate privacy protection in place (Braun et al., 2018). A recent study shows that 68% of the respondent's motivation for self-measurement with m-health apps would increase if there was strong privacy protection (Härkönen and Räsänen, 2021). In addition to the sensitivity of the data, another privacy-related subject that individuals are worried about is the unauthorized distribution of their data to third parties (Lidynia et al., 2019). It is often challenging for users to follow how the data will be used by AI-powered healthcare services and what sort of consequences it might generate (Trocin et al., 2021). For example, as mentioned earlier, Flo, the most popular period tracking app with over 100 million users, shared the extremely sensitive and intimate data of its users with Google and Facebook without their knowledge (Gupta and A., 2021). Providing transparent explanations about data gathering activities to users could enable them to make better and more confident choices (Van Kleek et al., 2017).

Previous studies show that users are increasingly concerned about their privacy and data security (Zhou et al., 2019). However, these concerns do not directly transfer into action, as people continue to act in a controversial way (Gerber et al., 2018). This sort of controversial behavior is known as personalization-privacy paradox (Guo et al., 2016). For example, users might state that they hold personal data privacy in high importance but simultaneously disclose too much personal information or agree to an app privacy policy without reading it. A recent report shows that approximately only half of the 4,000 respondents familiarized themselves with the terms of use of the m-health apps they used (Härkönen and Räsänen,

2021). While these controversial decisions can be due to users' lack of awareness about privacy issues, it remains unclear whether they really understand the extent of the required access to personal data or not (Van Kleek et al., 2017). A contributing factor that exacerbates the issue is that many apps do not actively raise the user's awareness nor offer transparent explanations regarding their data collection and use (Van Kleek et al., 2017). For instance, Polykalas and Prezerakos (2019) examined the correlation between over a thousand mobile apps requests for personal data and their subscription plans (i.e. free or paid), and concluded that free apps request access to personal data more extensively than paid apps.

2.3 Research Model and Hypotheses

2.3.1 Personalization

The personalization-privacy paradox emerges especially in the field of AI-powered services like m-health apps that collect vast amounts of sensitive information about the users and their daily lives. For example, Kang and Jung (2021) studied the personalization-privacy paradox among smartwatch users and identified three types of users. While a group of users was either interested in the benefits of wearables (i.e. benefit-oriented users) or concerned about their privacy risks (i.e. risk-oriented users), the biggest group of users (i.e. ambivalent users) had the highest level of perceived benefits and privacy concerns simultaneously (Kang and Jung, 2021). Previous research argue that often the perceived benefits of a service outweigh users' privacy concerns or the perceived risks of self-disclosure (Dienlin and Metzger, 2016). Guo et al. (2016) studied the personalization-privacy paradox among m-health users and found that the perceived level of personalization affects the intention to adopt the service positively, while the level of privacy concerns affects the adoption intention negatively. The paradox indicates the relationship between personalization and influences privacy concerns (Guo et al., 2016); as personalization levels increase, so will the level of privacy concerns of the user. Guo et al. (2016) found that trust can help balance the personalization-privacy paradox, indicating that customers with privacy concerns are less likely to adopt the services because they don't trust the service provider. Liu and Tao (2022) found that the more personalized a smart healthcare service was, the more trustworthy consumers considered it to be. The authors argue that this is because users feel that a more personalized service takes better into consideration their unique health conditions. Guo et al. (2016) also found that perceived personalization increases the likelihood of acquiring user trust. Based on these observations, we hypothesize that the level of personalization an app offers has an influence on users' privacy concerns and trust as well as their intention to continue using the app in the future (i.e. behavioral intention).

H1: *Personalization positively affects behavioral intention*

H2: *Personalization positively affects privacy concerns*

H3: *Personalization positively affects trust*

2.3.2 Privacy Concerns

Becker (2018) studied the information privacy concerns of health wearables users and found out that many users have accepted being constantly monitored, and they do not feel like they can do anything regarding privacy issues. Simultaneously, the users see the potential monetary benefits of providing their health data when dealing with insurance companies and thus believe that the benefits outweigh the risks (Becker, 2018). Another study by Zhou et al. (2019) shows that the majority of m-health app users who participated in the study were concerned about their privacy, and they would like the apps to have a set of features to diminish their privacy concerns. Lidynia et al. (2019) studied the perceived benefits and barriers of fitness apps and wearables and found that privacy concerns are among the biggest perceived barriers for users. In another paper, Lidynia et al. (2018) studied the privacy concerns and sensitivity regarding the data collection of the wearables, finding that people would rather keep their wearables data to themselves than share it with social networks or with companies. Privacy concerns impact users' self-disclosure intentions. Zhang et al. (2018) show that privacy concerns have a negative effect on information disclosure intentions in online health communities. Similarly, Keith et al. (2013) found that

increased perceived privacy risk decreases an individual's intention to disclose information on mobile devices. Lastly, privacy concerns and trust have an impact on each other. Users can be reluctant to share personal information or at least aim to disclose as little as possible, which is not in the best interest of the companies developing m-health services. If users perceive that their privacy is challenged by the app, it will negatively affect their trust in the app (Fox and Connolly, 2018, Liu and Tao, 2022). Therefore, we hypothesize:

H4: *Privacy concerns negatively affect behavioral intention*

H5: *Privacy concerns negatively affect self-disclosure*

H6: *Privacy concerns negatively affect trust*

2.3.3 Trust

As mentioned earlier, trust is a central theme when discussing citizens' adoption of smart health technologies, as the technologies need to have the user's trust for them to be inclined towards adopting them. Trust is found to be especially important in the early stage of an AI technology relationship (Liu and Tao 2022). To achieve trust, an individual should find the health service to be reliable and dependable in supporting the person's healthcare activity. For instance, in their study, Fox and Connolly (2018) found that trust in smart healthcare vendors reduces the user's health information privacy concerns. Liu and Tao (2022) found that trust significantly influenced a user's intention to adopt smart healthcare services. The more a person trusts healthcare services, the more likely it is they will use them. Krasnova et al. (2012) argue that trust in the service provider and in other users of social networking sites (SNS) is essential for self-disclosure, and thus trust acts as a mediator for self-disclosure. Anderson and Agarwal (2011) studied the impact emotions, context and trust have on users' willingness to disclose their health information by conducting a survey study among the US population. Regarding trust, they found that trust significantly increases an individual's willingness to share their health information.

H7: *Trust positively affects behavioral intention*

H8: *Trust positively affects self-disclosure*

2.3.4 Digital self-efficacy

Self-efficacy has been found to affect users' acceptance of technologies (Lidynia et al., 2018, Koivumäki et al., 2017, Chandrasekaran et al., 2020). Self-efficacy refers to a user's confidence in their ability to successfully perform a task or behavior, leading to the wished outcome (Koivumäki et al., 2017). As such, self-efficacy affects a person's intention to act (Zhang et al., 2018). Dienlin and Metzger (2016) studied the effect of privacy, self-efficacy, and self-disclosure on people's self-disclosure and self-withdrawal on SNS. They contemplated that perhaps users who feel that they have the skills needed to protect themselves by using, for example, privacy settings would also be more willing to disclose information. However, their results regarding this question were not found significant, so it remains to be further researched. In their study, Zhang et al. (2018) found that self-efficacy negatively affects privacy concerns. Raman and Pashupati (2004) found in their research that people with a higher level of self-perceived digital competency have privacy concerns, but they are well equipped to deal with them and understand the risk of having their information online. These people did not avoid using the internet but rather were cautious in their online behavior and took the preventive measures that they could, whereas people with a lower level of self-perceived digital competency had the highest levels of concern regarding their data privacy (Raman and Pashupati, 2004). Therefore, we hypothesize:

H9: *Digital self-efficacy has a positive effect on behavioral intention*

H10: *Digital self-efficacy positively affects self-disclosure*

H11: *Digital self-efficacy negatively affects privacy concerns*

2.3.5 Self-disclosure

M-health apps require a high level of self-disclosure from users to be able to offer them optimal, personalized service. Self-disclosure takes place when users share information about themselves (e.g. personal details, opinions, moods) with digital services. Based on this information, it is possible to make conclusions about a person's personality, habits, and performance (Krasnova et al., 2012). Self-disclosure is tightly related to the privacy calculus theory (Laufer and Wolfe, 1977), which suggests that users decision to disclose or retain information is based on their assessment of the possible benefits and risks that the information sharing might bring (Zhang et al., 2018). The privacy calculus explains that the level of self-disclosure depends on three influencing factors: privacy concerns, the anticipation of benefits, and trusting beliefs (Krasnova et al., 2012). These potential benefits can be, for example, personalization, enhancement in self-presentation, and enjoyment. Potential risks, on the other hand, might be different kinds of privacy violations (Zhang et al., 2018). The trade-off between privacy calculus and risk calculus also affects a user's self-disclosure intention. This means that if the benefit of sharing information about oneself exceeds the potential risks related to information sharing, users are often willing to share their personal information (Zhang et al., 2018). Previous studies have examined the antecedents of self-disclosure, but we lack an understanding of how self-disclosure affects behavioral intention. Therefore, we hypothesize that a higher level of self-disclosure intention would have a positive effect on m-health behavioral intention, as the users who tend to self-disclose more information about themselves has a higher tendency to start using m-health apps.

H12: *Self-disclosure has a positive effect on behavioral intention*

2.3.6 Anthropomorphism

Gavrilova and Kokoulina (2015) state that personalization and anthropomorphism are basic properties of smart technologies. Anthropomorphism refers to the phenomenon when human-like traits and behaviors are given to non-human creatures or objects (Epley et al., 2007). In the context of this study, anthropomorphism refers to the human-like characteristics of m-health services, which can be especially seen in chatbots like Woebot virtual therapist. There have been mixed results in previous research regarding the influence anthropomorphism has on technology adoption intention. Some findings indicate that human-like characteristics in AI provoke negative emotions within users, triggering feelings of unease or even a threat to the user's human identity. For example, Lu et al. (2019) found that in a hotel setting, a customer's intention to use an AI robot device was affected negatively by the robot's human-like characteristics. Coetzer et al. (2017) studied the impact that anthropomorphism and affective design have on the adoption intention of m-health services in rural communities. They found that anthropomorphism does have a positive impact on m-health adoption. Liu and Tao (2022) found in their research that anthropomorphism has a significant positive effect on the acceptance of smart healthcare services through trust. Therefore, following the findings of the studies conducted in the healthcare context we hypothesize that:

H13: *Anthropomorphism has a positive effect on trust*

2.3.7 Control variables

Previous research shows that demographic factors have an influence on individuals' privacy concerns and acceptance of m-health apps. Kang and Jung (2021) report that older users are more inclined to address the benefits of smart wearables than the privacy risks of using them. Zhao et al. (2018) argue that older people are more aware of health issues and thus might experience a bigger benefit of m-health apps. Previous research also shows that women are more concerned about privacy issues than men (Kang and Jung, 2021, Zhou et al., 2019, Tifferet, 2019) while trust plays a larger role in behavioral intention for women than men (Liu and Tao, 2022). The evidence regarding the impact of education level on privacy concerns in earlier research has been inconclusive. Some researchers have found that highly educated people are less concerned about privacy matters (Boerman et al., 2021), while others report that highly educated people have more privacy concerns as they have more knowledge about online data

privacy (O'Neil, 2001, Anderson and Agarwal, 2011). Based on these observations, we decided to examine the influence of users' age, gender, and education on the relationships in our model.

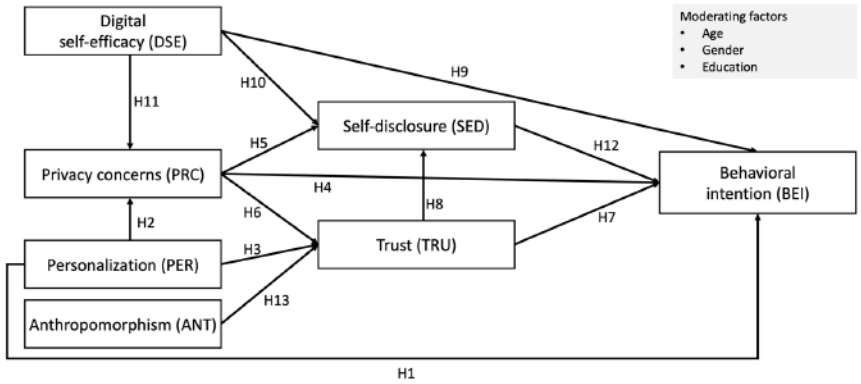

Figure 1. Research model

Figure 1 shows the theoretical model developed drawing on previous IS studies on users' privacy behaviors and concerns regarding m-health apps. In the following sections we discuss the key constructs of the model and their relationships.

3 Methodology

3.1 Data collection and respondents

The data was collected using an online survey targeting m-health app users. We distributed the survey through LinkedIn, Facebook, and Instagram. The survey answers were collected anonymously, and the participants were given information about the purpose and context of the study. The survey consisted of three parts. The first part was an explanation of the survey's background and purpose. Part two had five questions about the respondent's demographic information and the type of m-health apps they use. The third part consisted of questions related to the measurement scales. The survey was designed in English and translated into Finnish and Estonian to enable local citizens who do not speak English also answer the survey. The respondent demographics can be seen in a detailed summary in Table 1.

Demographics	Value	Number	Percentage
Age	18-30	181	72.69
	31-45	42	16.87
	46-60	21	8.43
	> 60	5	2.01
Gender	Female	151	60.64
	Male	95	38.15
	Non-binary/third gender	1	0.40
	Preferred not to say	2	0.80
Education	Highschool/vocational education	17	6.83
	Bachelor's degree	76	30.52
	Master's degree	131	52.61
	Doctoral degree	25	10.04

Table 1. Demographic statistics

3.2 Measures

We relied on previously tested scales suggested by previous studies to operationalize our constructs (see Appendix A). We used a 5-point Likert scale ranging from "Strongly disagree" to "Strongly agree" for all the items in the questionnaire. Behavioral intention was adopted from Venkatesh et al. (2003) and Personalization was adopted from Komiak and Benbasat (2006) and Smith et al. (2011). For Trust we used a three item scale suggested by Choi and Ji (2015) and for Self-disclosure we used the scale suggested by Bansal et al. (2010). We used a four item scale for Anthropomorphism (Lu et al., 2019) and a three item scale for Digital self-efficacy (Deng, 2013). Finally, Privacy concerns was adopted from (Zhang et al., 2019). When necessary, the questions were modified to suit the current study.

4 Data analysis and Results

We used partial least squares structural equation modelling (PLS-SEM) technique to analyze the data, since it is suitable for exploratory research (Gefen et al., 2011). The analysis was conducted using SPSS AMOS software. The survey generated 337 responses in total, out of which 249 were complete and were used for the analysis. This sample size is big enough and exceeds the minimum requirement to run the PLS analysis (Hair et al., 2011, Gaskin, 2021). To test a PLS-SEM model, first, the reliability and validity the measurement model is assessed and then, the structural model and hypotheses are tested.

4.1 Assessment of measurement model

4.1.1 Reliability

The measurement model was assessed for internal consistency reliability, convergent validity, and discriminant validity. A common criterion is that internal consistency reliability is satisfied if the composite reliability constructs and Cronbach's alpha exceed 0.7. For convergent validity, the loadings for the constructs should be above 0.7, and the Average Variance Extracted (AVE) should be above 0.5 (Hair et al., 2013, Bohr and Memarzadeh, 2020). To ensure discriminant validity, the square root of each construct's AVE should be larger than its correlation with other constructs (Fornell and Larcker, 1981).

Table 2: Properties of Latent Variables

	TRU	**SED**	**DSE**	**PRC**	**PER**	**ANT**	**BEI**
Trust (TRU)	**0.71**						
Self-disclousure (SED)	0.39	**0.9159**					
Digital self-efficacy (DSE)	0.70	0.456	**0.791**				
Privacy concerns (PRC)	-0.29	-0.234	-0.225	**0.8708**			
Personalization	0.33	0.419	0.353	0.026	**0.7204**		
Anthropomorphism (ANT)	0.02	0.042	-0.158	0.081	0.145	**0.7905**	
Behavioral Intention (BEI)	0.55	0.532	0.629	-0.145	0.408	0.033	**0.92**
CA	0.79	0.94	0.76	0.89	0.85	0.86	0.92
CR	0.745	0.940	0.768	0.903	0.842	0.868	0.922
AVE	0.508	0.839	0.626	0.758	0.519	0.625	0.855
CA = Cronbach's alpha; CR = Composite reliability; AVE = Average Variance Extracted; Square roots of AVE are shown in bold.							

4.1.2 Factor Analysis

We started the measurement model assessment by doing Exploratory Factor Analysis (EFA). First, we tested the reliability of each construct's observable variable sets separately (see Table 2 for the results). In the reliability screening process, the constructs Cronbach's Alpha must exceed 0.7 (Hair et al., 2013). Therefore, in the process observed variable DSE_3 had to be dropped due to having Cronbach's Alpha below the threshold (0.687<0.7), and by dropping it, the threshold increased to an acceptable level of 0.757. Next, we tested the factor structures, and found that BEI_2 was loading on the construct of Trust.

This cross-loading was eliminated by taking BEI_2 out of the analysis. Additionally, leaving BEI_2 out of the analysis increased its Cronbach's Alpha from 0.823 to 0.921. Continuing to do Confirmatory Factor Analysis (CFA) with the data modified from EFA. According to the guidelines provided by Gaskin (2021) the model fit was satisfactory. Reliability, convergent validity, discriminant validity, and the Fornell-Larcker criterion were established (Fornell and Larcker, 1981), and all the loadings were above the minimum threshold of 0.5.

Common method bias

When the data is collected using a single method, like an online survey in this case, it may produce a systematic response bias (Gaskin, 2021). To check for the Common Method Bias (CMB), we performed Harman's single factor test. We constrained the number of factors extracted to 1 and validated that one factor contributed to less than 50% (result 23%) of the total variance expected in the model. In addition to this, we checked for a Common Latent Factor (CFL) in SPSS AMOS software. After comparing the standard regression weights from the CLF model to the model without CLF, we could verify that there are very small differences between the standardized regression weights, smaller than 0.07, which indicates that a CMB is not an issue with the data.

4.2 Structural model assessment and hypotheses testing

The structural model was assessed in three parts. First, we tested the hypotheses presented in the study as direct effects. Second, we explored the direct, indirect, and mediating effects the latent variables have on behavioral intention. Third, we did multi-group analyses with the demographic variables in groups of two to explore the differences in results based on demographic differences.

*Table 3. Hypotheses testing results (Note: *** =p <0.001)*

Hypothesis: path	Coefficients	CR	p-value	Supported?
H1: Personalization -> Behavioral intention	0.091	1.323	0.186	No
H2: Personalization -> Privacy concerns	0.111	1.628	0.103	No
H3: Personalization -> Trust	0.439	5.358	***	Yes
H4: Privacy concerns -> Behavioral intention	0.053	0.845	0.398	No
H5: Privacy concerns -> Self-disclosure	-0.110	-1.680	0.094	No
H6: Privacy concerns -> Trust	-0.252	-3.63	***	Yes
H7: Trust -> Behavioral intention	0.202	2.672	0.008	Yes
H8: Trust -> Self-disclosure	0.244	3.505	***	Yes
H9: Digital self-efficacy -> Behavioral intention	0.414	5.575	***	Yes
H10: Digital self-efficacy -> Self-disclosure	0.314	4.330	***	Yes
H11: Digital self-efficacy -> Privacy concerns	-0.267	-3.670	***	Yes
H12: Self-disclosure -> Behavioral intention	0.279	4.236	***	Yes
H13: Anthropomorphism -> Trust	0.007	0.096	0.923	No

4.2.1 Hypotheses testing

The model was run on 500 bootstrap samples and at a bootstrap confidence level of 95. To examine the model fit we relied on the guidelines suggested by (Hu and Bentler, 1999, Gaskin, 2021). Regarding the model fit, the CMIN/DF (i.e. chi-square fit statistics/degree of freedom) was 2.527, indicating a good fit as the acceptable threshold is 3. The comparative fit index (CFI) of the model was 0.912, above the acceptable level of 0.9. The p-value is also in line with a value of 0.000. Finally, RMSEA (i.e. root mean square error of approximation) was 0.078 and within the acceptable threshold of 0.10. As shown in Table 3, the results of the PLS analysis show that the majority of hypotheses (8 out of 13) were supported, providing considerable support for the suggested research model. Personalization-privacy

paradox was observed, as, on the one hand, personalization was found to have a strong and significant positive effect on trust (H3) even though personalization did not have a significant positive effect on users' privacy concerns (H2) or behavioral intention (H1). On the other hand, privacy concerns had a significant negative effect on trust (H6) even though these privacy concerns did not have a significant negative effect on users' behavioral intention (H4) or self-disclosure intention (H5). Trust, however, did have a significant positive effect on users' behavioral intention (H7) and self-disclosure intention (H8). This confirms the role of trust in balancing users' privacy concerns and personalization preferences. In addition, the level of users' digital self-efficacy had a significant positive impact on both behavioral intention (H9) and self-disclosure (H10), while digital self-efficacy had a significant negative effect on the user's privacy concerns (H11). The user's self-disclosure intention had a significant positive effect on behavioral intention (H12), and lastly, anthropomorphism was not found to have a significant positive effect on trust (H13).

4.2.2 Direct, indirect, and mediating effects

Digital self-efficacy had the largest total effect on behavioral intention, with a total effect of 0.51. Self-disclosure and trust had a similar weight of total effect on the behavioral intention with effects of 0.28 and 0.27. Additionally, personalization had a total effect of 0.2 on behavioral intention, even though the direct effect of personalization on behavioral intention was insignificant. From the constructs, only privacy concerns and anthropomorphism were not found to have a significant total effect on behavioral intention. Next, we tested the mediating effects of privacy concerns, self-disclosure, and trust to see how they affect behavioral intention. It was found that self-disclosure and privacy concerns partially mediate the positive effect of self-efficacy on behavioral intention. Trust fully mediated the relationships from personalization and privacy concerns to behavioral intention.

4.2.3 Multi-group analysis

We performed a multi-group analysis to test whether the relationships hypothesized in the model vary for different control variables. Since multi-group analysis can be performed only in groups of two in SPSS AMOS, aside from gender (male vs. female), we recoded the rest of the demographic variables to analyze them in groups of two, age (younger vs. older) and education (lower vs. higher education). First, we tested the impact of gender, male (n=95) vs. female (n=151), on the hypotheses. There were some differences between genders and in the outcome in general. For female respondents, the level of personalization did have a significant positive effect on the level of privacy concerns (H2), but for male respondents, the effect was negative (yet not significant), creating a big difference between the two groups' path coefficients (0.5). For males, the level of personalization did not have a significant positive effect on trust (H3), and the level of privacy concerns did have a significant negative effect on the level of self-disclosure (H5). Also, H8, H11, and H12 were found not to be significant for the male group.

For age, we divided the participants into two age groups: 1) Younger adults, consisting of 18-30 years old respondents (n= 181), and 2) Older adults, all the respondents above 30 years old (n=68). In the younger group, personalization had a significant positive effect on behavioral intention (H1). For the older group, privacy concerns did not have a significant negative effect on trust (H6), and H11 and H12 were not supported, even though they were supported in the younger and general groups. For education, we created two groups: (1) lower education (n=93) containing high school and Bachelor's degrees and (2) higher education (n=156) containing Master's and Doctoral degrees. Some differences between the general test and education-specific tests were found. For lower education group, personalization did have a significant effect on privacy concerns, whereas, in the general group and higher education group, such an effect was not found (H2). For the higher education group, privacy concerns were found to have a significant negative effect on self-disclosure, which is a relationship not found in the general group or lower education group (H5). Privacy concerns were not found to have a significant negative effect on trust in the lower education group (H6). Trust did not have a positive effect on self-disclosure in the higher education group (H8). H9 and H12 were also not supported in the lower education group.

5 Discussion

In this study, we examined how users' privacy concerns and the level of personalization provided by m-health apps influence users trust in the apps as well as their intention to use and disclose personal information with m-health apps. The results indicate that privacy concerns do not directly have a negative effect on the user's behavioral intention toward m-health apps. However, privacy concerns have a significant negative effect on users' trust towards m-health apps, and trust, in turn, has a significant positive effect on users' behavioral intention. Even though, the level of personalization did not significantly increase users' privacy concerns or behavioral intention, the personalization-privacy paradox was still present. among the sample especially, because personalization was found to have a significant positive effect on trust, while trust was found to fully mediate a slight negative effect of privacy concerns on behavioral intention. These findings are in line with the findings of previous studies (Guo et al., 2016; Liu and Tao, 2022) that show the role of trust in balancing personalization-privacy paradox. This could imply that users consider more personalized m-health services to be more trustworthy and therefore they feel less concerned about potential privacy issues that might occur from using and sharing personal information with these apps. Nevertheless, our respondents still had privacy concerns about whether the m-health apps were using their personal information or sharing it with other entities without authorization.

5.1 Theoretical contributions

Our study makes several new contributions to IS research, especially the m-health and privacy literature. First, our study provides a more nuanced understanding of personalization-privacy paradox in the context of m-health apps, especially in contrast to studying smart healthcare applications in general (Liu and Tao, 2022).. Our results show that m-health users' privacy concerns do not have a significant negative effect on their self-disclosure intention nor behavioral intention, as users trust m-health apps that provide a higher level of personalization. These findings confirm the personalization-privacy paradox (Guo et al., 2016; Liu and Tao, 2022), while being contrast to the findings of previous studies suggesting privacy concerns have a negative effect on user's information disclosure (Keith et al., 2013, Zhang et al., 2018) and being the number one barrier in smart health adoption (Lidynia et al., 2019). Our study further shows that the magnetite of privacy paradox is influenced by users' level of digital self-efficacy. Digital self-efficacy was found to decrease users' privacy concerns while increasing their intention to share personal information with m-health apps. This indicates that users who consider themselves digitally savvy are more likely to disclose their information despite their privacy concerns, perhaps because they feel more confident that they can take the needed measures to protect their privacy.

Second, our multi-group analyses provide a better understanding of how different demographic factors, especially gender and education affect the magnetite of personalization-privacy paradox among m-health users. Guo et al. (2016) have only examined the role of age differences on users' behavioral intention and called for future studies to focus on other demographic differences. Our results show that personalization-privacy paradox is influenced by gender, age, and level of education. In terms of gender, the level of personalization increased females' privacy concerns significantly, but the influence was not significant for men. This is in line with previous studies suggesting that women tend to have more privacy concerns than men (Zhou et al., 2019, Liu and Tao, 2022, Tifferet, 2019). At the same time, privacy concerns had only a significant negative effect on self-disclosure in the male group. This indicates that the personalization-privacy paradox is stronger for females than males, as females were found to have more privacy concerns but simultaneously were more inclined towards personalized m-health services and a higher level of self-disclosure. Regarding the age, for older users' self-disclosure intention did not have a significant effect on behavioral intention. This may indicate that disclosing personal information for getting more personalized services does not play an important role among older adults, compared to younger adults. However, our results show that personalization has a significant positive effect on the behavioral intention of the younger group, indicating that younger users truly value m-health apps' personalized services. Finally, in terms of education, users with a higher level of education acted more accordingly to their privacy concerns. These findings are in line with the findings

reported by previous studies (e.g. (Anderson and Agarwal, 2011). However, privacy concerns did not have a negative effect on behavioral intention in the higher education group either. The largest difference in path coefficients was found in the path between trust and self-disclosure, with a substantial positive effect in the lower education group, indicating that with a higher level of trust, the lower education group is more prone to increase their level of self-disclosure.

Finally, our study shows that the level of self-disclosure has a positive effect on users' intention to use m-health apps. This could indicate that people who are more willing to share personal information, are more likely to use m-health apps and perhaps other personalized services. The effect of the level of self-disclosure on behavioral intention had not been tested in previous studies (e.g. Guo et al., 2016); rather, the factors affecting users' self-disclosure have been studied (e.g. see (Krasnova et al., 2012)).

5.2 Practical Implications

An important practical question is how companies could perform better in the m-health field to attract and retain users with m-health applications, realizing the potential benefits of the apps for both individuals and society at large. Some researchers suggest that companies should provide users easy access to their data and strong privacy protection (Härkönen and Räsänen, 2021). However, based on our results, we suggest that companies should consider the age and gender of their target users when designing the personalization and privacy preferences of their applications. For instance, our results shows that younger users highly value and trust personalized m-health apps. In addition, our results show that while women tend to have more privacy concerns than men, they tend to trust and disclose more health information with highly personalized m-health services.

M-health apps encourage individuals to take better care of their personal health and well-being, acting as a preventive manner for lifestyle diseases. Our study shows that digital self-efficacy plays an important role in using m-health apps. Younger people (i.e. digital natives) often have higher levels of digital self-efficacy, enabling them to use m-health apps easier. However, older people who would benefit more from using m-health apps often lack the necessary digital skills for using these apps. Therefore, we argue that it is important to improve citizens' digital skills and competencies, especially the elderly, to ensure that all citizens and the society at large benefit from using m-health apps and other public digital services. Lastly, trust plays a central role in encouraging citizens to share their personal health information with m-health apps. Thus, m-health service providers must establish trust to facilitate m-health app adoption and for users to fully adopt and enjoy personalized services.

5.3 Limitations and future work

The study naturally has some limitations. First, the survey sample might suffer from a sampling bias, especially in the form of non-response and under-coverage bias. Naturally, it can be expected that people who are active users of m-health apps were more inclined to answer the survey than people who do not use m-health apps. Therefore, our observations do not reflect the perceptions of the people who do not use m-health apps. In addition, most of our respondents were between 15-45 years old and female, therefore, other genders and elderly groups were underrepresented in the sample. Furthermore, in this study we explored personalization-privacy paradox in the use of m-health apps in general. Future research could study even a more niche segment of the well-being m-health app category, such as femtech or mental health apps. While their market share is growing rapidly, these kinds of apps deal with the most sensitive personal information about users. Therefore, privacy and trust issues might be even more prevalent in their use, and these kinds of apps need to be very personalized to deliver value to the user. As discussed earlier, our results show that demographic factors and level of digital skills influence individuals' privacy concerns and trust and as well as the adoption of m-health services. For instance, the personalization-privacy paradox was more common among female respondents. These findings are especially valuable considering the increasing popularity of femtech applications that collect sensitive maternal and menstrual health information. Therefore, the personalization-privacy paradox deserves further investigation by researchers and practitioners that focus on femtech or gender issues in developing and using mobile applications. Finally, in this study we used PLS-SEM to explore

the interrelationship between users' privacy concerns, personalization preferences, and their digital self-efficacy and their influence on users' intention to use and disclose personal information to apps. Future studies can use experiment design or qualitative approaches to examine the causal relationships between these constructs and provide us with a deep understanding of how users balance their privacy concerns and personalization preferences.

6 Conclusions

In this study, we set to examine how users' digital competencies and interest in personalized services on the one hand and their privacy concerns and trust in a service on the other hand affect their intention to use and disclose personal health information with m-health apps. To that end, we conducted an online survey to explore personalization-privacy paradox and its related concepts in the m-health context. Our results confirm that while users claim to have privacy concerns about using m-health apps, these concerns do not affect their intention to use and share personal information with these apps. The magnitude of this personalization-privacy paradox was influenced by gender, age, and education levels as well as the respondents' levels of digital self-efficacy. However, future research is needed to examine the reasons and mechanism underlying these associations. Finally, our results show that trust play an important role in balancing users privacy concerns and their personalization preferences and ultimately facilitating users' intention to use m-health apps and share personal health information with these apps.

Acknowledgments

This study has been partly supported by the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 856602.

Appendix A: Questionnaire items

Construct (Source)	Items	Load
Behavioral intention (Venkatesh et al., 2003)	I intend to continuously use m-health services in the future (BEI_1)	0.93
	I would use m-health services more frequently in the future (BEI_2)	---
	I plan to continuously use m-health services in the future (BEI_3)	0.92
Trust (Choi & Ji, 2015)	M-health services are dependable (TRU_1)	0.50
	M-health services are reliable (TRU_2)	0.68
	Overall, I can trust m-health services (TRU_3)	0.90
Personalization (Komiak & Benbasat 2006; Smith et al 2011)	M-health services provide personalized services that are based on my information (PER_1)	0.74
	M-health services personalize my health management experience (PER_2)	0.82
	M-health services personalize my health management by acquiring my personal preferences (PER_3)	0.78
		0.62
	M-health services personalize and deliver healthcare services to me according to my information (PER_4)	0.63
	M-health services deliver personalized healthcare services (PER_5)	
Self-disclosure (Bansal et al., 2010)	I am likely to reveal my health information in m-health services (SED_1)	0.94
	I will probably reveal my health information in m-health services (SED_2)	0.96
	I am willing to reveal my health information in m-health services (SED_3)	0.84
Anthropomorphism (Lu et al., 2019)	M-health services have consciousness (ANT_1)	0.66
	M-health services have a mind of their own (ANT_2)	0.89
	M-health services have their own free will (ANT_3)	0.84
	M-health services will experience emotions (ANT_4)	0.75
Digital self-efficacy (Deng, 2013)	I would be confident in using m-health services even if there was no one around to show me how to use them (DSE_1)	0.71
	I feel confident managing my health with m-health services (DSE_2)	0.87
	I have the skills necessary to learn and use the m-health services (DSE_3)	---
Privacy concerns (Zhang et al., 2019)	I am concerned that m-health services will collect too much personal information from me (PRC_1)	0.71
	I am concerned that m-health services will use my personal information for other purposes without my authorization (PRC_2)	0.97
	I am concerned that m-health services will share my personal information with other entities without my authorization (PRC_3)	0.91

References

ANDERSON, C. L. & AGARWAL, R. (2011). The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information. *Information Systems Research,* 22**,** 469-490.

BANSAL, G., ZAHEDI, F. M. & GEFEN, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems,* 49**,** 138-150.

BECKER, M. (2018). Understanding Users' Health Information Privacy Concerns for Health Wearables. *Hawaii International Conference on System Sciences*.

BOERMAN, S. C., KRUIKEMEIER, S. & ZUIDERVEEN BORGESIUS, F. J. (2021). Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel Data. *Communication Research,* 48**,** 953-977.

BOHR, A. & MEMARZADEH, K. (2020). The rise of artificial intelligence in healthcare applications. *Artificial Intelligence in Healthcare.* Elsevier.

BRAUN, T., FUNG, B. C. M., IQBAL, F. & SHAH, B. (2018). Security and privacy challenges in smart cities. *Sustainable Cities and Society,* 39**,** 499-507.

CHANDRASEKARAN, R., KATTHULA, V. & MOUSTAKAS, E. (2020). Patterns of Use and Key Predictors for the Use of Wearable Health Care Devices by US Adults: Insights from a National Survey. *Journal of Medical Internet Research,* 22**,** e22443.

CHOI, J. K. & JI, Y. G. (2015). Investigating the Importance of Trust on Adopting an Autonomous Vehicle. *International Journal of Human-Computer Interaction,* 31**,** 692-702.

COETZER, J., GROBBELAAR, L. & MASINDE, M. E. (2017). Making software humane: the effects of affective and anthropomorphism on the adoption of an m-health application. *The South African Institute of Computer Scientists and Information Technologists*. Thaba 'Nchu, South Africa, 1-8.

COOK, D. J., DUNCAN, G., SPRINT, G. & FRITZ, R. L. (2018). Using Smart City Technology to Make Healthcare Smarter. *Proceedings of the IEEE,* 106**,** 708-722.

DIENLIN, T. & METZGER, M. J. (2016). An Extended Privacy Calculus Model for SNSs: Analyzing Self-Disclosure and Self-Withdrawal in a Representative U.S. Sample: THE EXTENDED PRIVACY CALCULUS MODEL FOR SNSs. *Journal of Computer-Mediated Communication,* 21**,** 368-383.

EPLEY, N., WAYTZ, A. & CACIOPPO, J. T. (2007). On seeing human: a three-factor theory of anthropomorphism. *Psychological review,* 114**,** 864.

FORNELL & LARCKER (1981). Structural Equation Models with Unobservable Variables and Measurement Error: Algebra and Statistics. *STRUCTURAL EQUATION MODELS***,** 8.

FOX, G. & CONNOLLY, R. (2018). Mobile health technology adoption across generations: Narrowing the digital divide. *Information Systems Journal,* 28**,** 995-1019.

GASKIN, J. (2021). *Statwiki* [Online]. Available: http://statwiki.gaskination.com/ [Accessed 29.09.2022].

GAVRILOVA, T. & KOKOULINA, L. (2015). Smart Services Classification Framework. *Federated Conference on Computer Science and Information Systems*, 203-207.

GEFEN, D., RIGDON, E. E. & STRAUB, D. (2011). Editor's comments: an update and extension to SEM guidelines for administrative and social science research. *MIS Quarterly***,** iii-xiv.

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.

GUO, X., ZHANG, X. & SUN, Y. (2016). The privacy–personalization paradox in mHealth services acceptance of different age groups. *Electronic Commerce Research and Applications,* 16**,** 55-65.

GUPTA, H. & A., S. N. (2021). Your App Knows You Got Your Period. Guess Who It Told?

HAIR, J. F., RINGLE, C. M. & SARSTEDT, M. (2011). PLS-SEM: Indeed a Silver Bullet. *Journal of Marketing Theory and Practice,* 19**,** 139-152.

HAIR, J. F., RINGLE, C. M. & SARSTEDT, M. (2013). Partial Least Squares Structural Equation Modeling: Rigorous Applications, Better Results and Higher Acceptance. *Long Range Planning,* 46**,** 1-12.

HÄRKÖNEN & RÄSÄNEN (2021). There is strong demand for wellbeing applications but where are the services Available: https://www.sitra.fi/en/blogs/there-is-strong-demand-for-well-being-applications-but-where-are-the-services/

HU, L. T. & BENTLER, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal,* 6**,** 1-55.

JIANG, F., JIANG, Y., ZHI, H., DONG, Y., LI, H., MA, S., WANG, Y., DONG, Q., SHEN, H. & WANG, Y. (2017). Artificial intelligence in healthcare: past, present and future. *Stroke and Vascular Neurology,* 2**,** 230-243.

KANG, H. & JUNG, E. H. (2021). The smart wearables-privacy paradox: A cluster analysis of smartwatch users. *Behaviour & Information Technology,* 40**,** 1755-1768.

KAO, C.-K. & LIEBOVITZ, D. M. (2017). Consumer Mobile Health Apps: Current State, Barriers, and Future Directions. *PM&R,* 9**,** S106-S115.

KEITH, M. J., THOMPSON, S. C., HALE, J., LOWRY, P. B. & GREER, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies,* 71**,** 1163-1173.

KOIVUMÄKI, T., PEKKARINEN, S., LAPPI, M., VÄISÄNEN, J., JUNTUNEN, J. & PIKKARAINEN, M. (2017). Consumer Adoption of Future MyData-Based Preventive eHealth Services: An Acceptance Model and Survey Study. *Journal of Medical Internet Research,* 19**,** e429.

KOMIAK & BENBASAT (2006). The Effects of Personalization and Familiarity on Trust and Adoption of Recommendation Agents. *MIS Quarterly,* 30**,** 941.

KOTZ, D., GUNTER, C. A., KUMAR, S. & WEINER, J. P. (2016). Privacy and Security in Mobile Health: A Research Agenda. *Computer,* 49**,** 22-30.

KRASNOVA, H., VELTRI, N. F. & GÜNTHER, O. (2012). Self-disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture: Intercultural Dynamics of Privacy Calculus. *Business & Information Systems Engineering,* 4**,** 127-135.

KUKAFKA, R. (2019). Digital Health Consumers on the Road to the Future. *Journal of Medical Internet Research,* 21**,** e16359.

LAUFER, R. S. & WOLFE, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues,* 33**,** 22-42.

LIDYNIA, C., BRAUNER, P. & ZIEFLE, M. (2018). A Step in the Right Direction – Understanding Privacy Concerns and Perceived Sensitivity of Fitness Trackers. *In:* AHRAM, T. & FALCÃO, C. (eds.) *Advances in Human Factors in Wearable Technologies and Game Design.* Cham: Springer International Publishing.

LIDYNIA, C., SCHOMAKERS, E.-M. & ZIEFLE, M. (2019). What Are You Waiting for? – Perceived Barriers to the Adoption of Fitness-Applications and Wearables. *In:* AHRAM, T. Z. (ed.) *Advances in Human Factors in Wearable Technologies and Game Design.*

LIU, K. & TAO, D. (2022). The roles of trust, personalization, loss of privacy, and anthropomorphism in public acceptance of smart healthcare services. *Computers in Human Behavior,* 127**,** 107026.

LU, L., CAI, R. & GURSOY, D. (2019). Developing and validating a service robot integration willingness scale. *International Journal of Hospitality Management,* 80**,** 36-51.

MATHENY, M. E. (2019). Artificial Intelligence in Helathcare -A Report From the National Academy of Medicine. *The Journal of the American Medical Association,* 323**,** 2.

MESKÓ, B., HETÉNYI, G. & GUORFFY, Z. (2018). Will artificial intelligence solve the human resources crisis in healthcare? *BMC Health services reserach***,** 545.

O'NEIL, D. (2001). Analysis of Internet Users' Level of Online Privacy Concerns. *Social Science Computer Review,* 19**,** 17-31.

PAPAGEORGIOU, A., STRIGKOS, M., POLITOU, E., ALEPIS, E., SOLANAS, A. & PATSAKIS, C. (2018). Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice. *IEEE Access,* 6**,** 9390-9403.

POLYKALAS, S. E. & PREZERAKOS, G. N. (2019). When the mobile app is free, the product is your personal data. *Digital Policy, Regulation and Governance,* 21**,** 89-101.

RAMAN, P. & PASHUPATI, K. (2004). Online Privacy: The Impact of Self Perceived Technologicl Competence. *Enhancing Knowledge Development in Marketing*, 5(1), 26-27.

SMITH, DINEV & XU (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly,* 35**,** 989.

TIFFERET, S. (2019). Gender differences in privacy tendencies on social network sites: A meta-analysis. *Computers in Human Behavior,* 93**,** 1-12.

TROCIN, C., MIKALEF, P., PAPAMITSIOU, Z. & CONBOY, K. (2021). Responsible AI for Digital Health: a Synthesis and a Research Agenda. *Information Systems Frontiers*.

VAN KLEEK, M., LICCARDI, I., BINNS, R., ZHAO, J., WEITZNER, D. J. & SHADBOLT, N. (2017). Better the Devil You Know: Exposing the Data Sharing Practices of Smartphone Apps. *CHI Conference on Human Factors in Computing Systems*. Denver Colorado USA, 5208-5220.

VENKATESH, MORRIS, DAVIS & DAVIS (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly,* 27**,** 425.

WHO (2019). WHO guideline: recommendations on digital health interventions for health system strengthening.

ZHANG, T., TAO, D., QU, X., ZHANG, X., LIN, R. & ZHANG, W. (2019). The roles of initial trust and perceived risk in public's acceptance of automated vehicles. *Transportation Research Part C: Emerging Technologies,* 98**,** 207-220.

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**,** 482-493.

ZHAO, Y., NI, Q. & ZHOU, R. (2018). What factors influence the mobile health service adoption? A meta-analysis and the moderating role of age. *International Journal of Information Management,* 43**,** 342-350.

ZHOU, L., BAO, J., WATZLAF, V. & PARMANTO, B. (2019). Barriers to and Facilitators of the Use of Mobile Health Apps From a Security Perspective: Mixed-Methods Study. *JMIR mHealth and uHealth,* 7**,** e11223.