Privacy Concerns regarding Wearable IoT Devices: How it is Influenced by GDPR?

Chinju Paul
Iowa State University
cpaul@iastate.edu

Kevin P Scheibe
Iowa State University
kscheibe@iastate.edu

Sree Nilakanta
Iowa State University
nilakant@iastate.edu

Abstract

Internet of Things (IoT) devices have implications for health and fitness. Fitness wearables can promote healthy behavior and improve an individual's overall health and quality of life. Even though fitness wearables have various benefits, privacy concerns regarding the data collected remain as a major barrier to adoption of fitness wearables. Intrinsic factors like disposition to value privacy and extrinsic factors like privacy policies and General Data Protection Regulation (GDPR) can influence users' privacy concerns. This research uses experimental design to understand how these factors influence privacy concerns. The results suggest that GDPR reduces the average privacy concerns of users. The study also shows that higher perception of effectiveness of privacy policy reduces the perception of privacy risks and increases the perception of privacy control. This study illustrates the effect of users' perceptions on factors like privacy policy, privacy control and GDPR on mitigating privacy concerns.

1. Introduction

Usage of smart devices and Internet of Things (IoT) devices have increased with the advancement of technology and extensive availability of network services. Wearable IoT devices are a group of IoT devices that can be worn on your body and available in the form of wristband sensors, smartwatches, glasses, head bound devices, etc. They have implications for the fields of health and medicine, fitness, transportation, enterprise, finance, gaming, and music [25]. Fitness wearables are one of the most common forms of wearables. Interventions through wearable activity trackers have shown to increase physical activity and promote healthy behavioral changes [15].

Although IoT devices have various benefits, some barriers prevent their adoption. One of the most prominent barriers to the widespread adoption of IoT is privacy concerns regarding the data collected. Data collected by IoT can be useful to the user in giving personalized services and

suggestions. However, the data is stored and analyzed by the provider (the company that provides services) which can lead to concerns about how data is managed. Studies by Hossain et al. [11] and Schierz, et al. [21] illustrated that privacy concerns negatively influence technology adoption. More specifically, Coughlan et al. [4] suggested that the privacy associated with data collected by IoT devices would negatively affect their adoption.

Our study analyses users' perceived privacy risks and concerns regarding wearables and how it is affected by antecedents like disposition to value privacy, privacy policies, and regulations. A better understanding of privacy concerns is important for the design of privacy-enhanced devices and policies. Regulations like GDPR can reduce users' privacy concerns by providing clear guidance, transparency and control on data management. Our study also tries to understand the effectiveness of privacy policies and GDPR in mitigating the privacy concerns of users. How privacy policies and GDPR can mitigate privacy concerns is not well studied in the context of IoT and this study attempts to fill this research gap.

2. Conceptual Background

There are a few studies that examined privacy concerns and their outcomes. According to Dinev and Hart [6], privacy concerns are an individual's anxiety regarding the potential loss of privacy due to willing or unwilling revelation of personal information. Smith, et al. [23] give an interdisciplinary review of privacy-related research. Most of the prior literature focus on privacy concerns of information collected online [22, 9, 6] and location-based privacy [31, 29, 19]. In addition, Xu et al. [29] extended the privacy calculus model by including personality characteristics (previous privacy experience, coupon proneness, and personal innovativeness) and different methods of personalization (covert and overt) for location-aware marketing. Also, Gopal et al. [9] studied how privacy concerns affect the intention to provide information for online services.

Concerns about privacy of IoT devices, however, are different from those of online transaction information and location information. This results from differences in the type, variety, and amount of data collected by the IoT device. Based on the type of IoT device, various forms of data are collected, including private data like heart rate, pulse, and other health-related data from fitness wearables; visual data from home security systems; recorded speech from home automation systems; energy usage patterns from smart energy meters; and location from mobile IoT devices. Because of the nature of the data collected by IoT devices, users' concerns and perceived risks about privacy might be different and the effects might be more exaggerated in the case of IoT.

A few studies have also identified privacy concerns as a barrier to IoT adoption. For instance, Coughlan et al. [4] studied the factors affecting the acceptance of home-based IoT technologies, and Canhoto and Arp [3] have analyzed the factors that influence the adoption and sustained use of wearables. Even though these studies identified privacy issues as a barrier, they did not explore the actual concerns of users and the factors influencing these concerns. Additionally, Prasad, et al. [20] tried to understand what influences the information sharing preferences and behavior of users of mHealth devices. This study tried to identify some of the privacy concerns of users on sharing their fitness information with others (family, friends, and public). Even though this study gave a preliminary understanding of privacy concerns, the study focused only on information sharing behavior which can be completely controlled by the user. In addition, Motti and Caine [16] explored the privacy concerns related to different kinds of wearables based on comments from online sources. Although online comments can provide some idea about privacy concerns, online comments and reviews mostly follow a bimodal distribution due to extremely negative or positive experiences [12]. Hence, online comments provide only a limited understanding of privacy concerns. Also, these studies did not consider the antecedents of privacy concerns like personality traits.

In summary, privacy concerns can be better understood by identifying users' perceptions of privacy risks associated with the use of IoT and identifying other antecedents to privacy concerns. This study tries to fill this gap in the existing literature. Xu, et al. [28] examined how industry regulation and privacy policy affects privacy concerns in the context of the internet. Xu, et al. [30] also studied the effects of individual self-protection, industry regulation and government policies on privacy concerns in the context of location-based services. We extend these two studies in the context of IoT to see how industry privacy assurance through regulation (GDPR) and privacy policy affects privacy concerns. One of the main contributions of our study is to provide an understanding of how privacy policy and regulations can mitigate privacy concerns regarding wearable IoT.

3. Privacy Policy, GDPR and Privacy Concerns

Privacy concerns related to the data collected by fitness wearables can be a significant barrier for the adoption of the wearable. A privacy policy is one of the possible ways by which an organization can address users' privacy concerns. Although this may be true, in the past, most of the privacy policies and terms and conditions provided were not very comprehensible and transparent. As a result, such a policy may not be effective in mitigating the user's privacy concerns. GDPR is a regulation in the European Union (EU) data protection law, which was approved in 2016 and was implemented in 2018. Even though GDPR was implemented in the EU, international organizations may follow some of the GDPR recommendations worldwide. As a result, GDPR can be effective even outside of the EU, including the United States. Policy revisions made by organizations based on GDPR recommendations are more comprehensible and transparent. These revised or new policies use examples to explain complex ideas and clearly explain how and what data are collected, who can access the data, how the data is used, how long the data is retained, and whether the user can delete the data. Such a clear and transparent policy might mitigate some of the privacy concerns of users.

A user may not read the privacy policy carefully enough, and hence the policy alone may not reduce privacy concerns because most privacy policies are long. On the contrary, if an organization declares that it complies with the recommendations of GDPR, it may reduce users' privacy concerns. A user may believe that conforming to a regulation like GDPR can enforce data protection and hence an organization may not practice opportunistic behavior due to the consequences associated with it. Hence GDPR act as an assurance to protect users' privacy. In short, our research tries to answer the following questions: how can we reduce privacy concern? Can a regulation like GDPR lower privacy concerns? We examine whether organizations' GDPR compliance will reduce users' privacy concerns.

4. Theoretical Foundation and Research Model

Interest in privacy has led to an extensive stream of privacy research in information systems literature and therefore, there are various models to explain how privacy concerns affect users' behavioral intentions. However, a complete review of all models is beyond the scope of this paper. The scope of this study is to understand the factors that affect privacy concerns. We use the APCO (Antecedents-Privacy Concerns-Outcomes) model, the privacy-calculus and the personalization-privacy paradox for our model development. The APCO model is a generalized model and suggests that there are antecedents to privacy concerns – like personality traits, regulations and so on – and in fact, privacy concerns have some outcomes like behavioral intentions [23, 7]. The privacy calculus and the personalization-privacy paradox can be used to explain how privacy concerns affect behavioral intentions. According to the privacy calculus model [5], an individual's decision to provide information depends on a risks-benefits analysis. Similarly, the personalization-privacy paradox is also based on the risks-benefits analysis [2].

4.1.   Perceived Privacy Risks

Perceived risks, in general, are an individual's belief in the possibility of uncertain adverse events from the use of a product or service [14]. Likewise, perceived privacy risks are beliefs about the uncertainty regarding adverse outcomes of loss of privacy due to the possibility of opportunistic behavior by others. Sensitivity to information sharing and privacy is a personality trait and can vary among individuals. As a result, some individuals are more willing to share information than others. Disposition to value privacy indicates an individuals' need to maintain boundaries that preserve their personal information [28]. An individual with a higher disposition to value privacy is more sensitive and may perceive more risks.
H1a: Disposition to value privacy positively affects perceived privacy risks.

On the other hand, if an individual considers that the privacy policy of the provider is effective, some of the concerns regarding the opportunistic behavior can be mitigated. Hence, if individuals perceive a privacy policy as effective, it will reduce their perceived privacy risks.
H1b: Perceived effectiveness of privacy policy negatively affects perceived privacy risks.

4.2.   Perceived Control

Perceived control in the context of privacy is a person's belief in his/her ability to control the release and diffusion of his/her personal information [28]. The collection, monitoring, and sharing of users' personal information can lead to a perception

of loss of control over the dissemination of their information [1]. Perception of control can be affected by a user's disposition to value privacy. An individual with a higher disposition to value privacy is more sensitive to information sharing and would demand higher control. Consequently, individuals with a higher disposition to value privacy would have reduced perception of control.
H2a: Disposition to value privacy negatively affects perceived control.

Perception of loss of control is considered as a threat by an individual. Privacy policy regarding the collection, use, and sharing of data collected will give the user more information and therefore would perceive better control. Given that, individuals who perceive that the privacy policy is effective will have a higher perception of control.
H2b: Perceived effectiveness of privacy policy positively affects perceived control

4.3.   Privacy Concerns

Information privacy is an individual's (or group's) right to decide when, how, and to what extent to share their information with others [27]. According to the communication privacy management theory [18], the cognitive process involving evaluation of perceived privacy controls and perceived privacy risks forms privacy concerns [28]. Perceived risks make an individual believe that there is higher uncertainty regarding the negative consequences of using a product or service [8]. Thus, an individual perceiving higher risks to privacy will have more concern about privacy.
H3a: Perceived privacy risks positively affects privacy concerns

Perception of control over the data collected by the IoT device is important regarding privacy concerns. Loss of control is considered a degree of helplessness by the user [24], and this increases the concerns. In brief, positive feeling of control will reduce privacy concerns.
H3b: Perceived control negatively affects privacy concerns

4.4.   Behavioral Intentions

Many studies have shown that privacy concerns affect behavioral intentions like intent to adopt and intent to use [31, 22, 14, 26, 19]. According to the APCO model, privacy concerns negatively influence behavioral intentions. Culnan and Armstrong [5] suggested that before disclosing personal information, a privacy calculus takes place when users evaluate the perceived benefits of information disclosure against the privacy concerns. Thus, the effect of privacy concerns on behavioral intentions is moderated by perceived benefits.

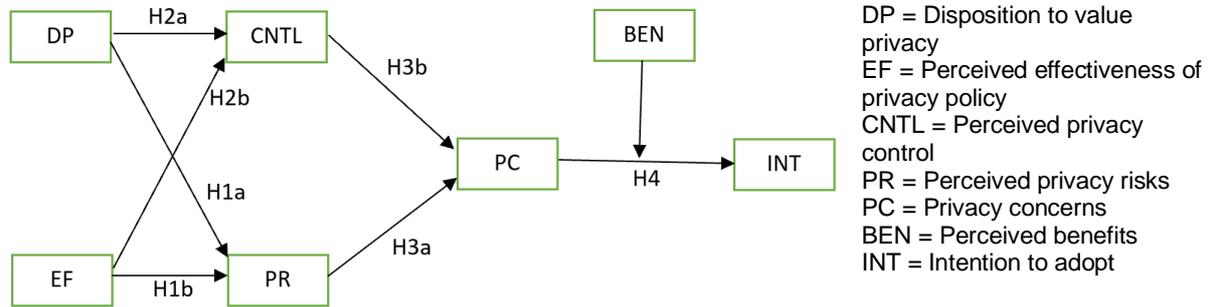*H4: Privacy concerns negatively affects behavioral intentions and is moderated by perceived benefits*

DP = Disposition to value privacy
EF = Perceived effectiveness of privacy policy
CNTL = Perceived privacy control
PR = Perceived privacy risks
PC = Privacy concerns
BEN = Perceived benefits
INT = Intention to adopt

Figure 1. Overall theoretical model

5. Data Collection

We conducted an experiment to study how a regulation like the GDPR influences the privacy concerns of the user. In this experiment, we are testing a part of research model involving antecedents to privacy concerns (figure 2).

5.1. Experiment

This experiment is aimed to analyze how GDPR influences users' perception of privacy concerns. If an organization is GDPR compliant, they are expected by the regulation to follow certain guidelines provided by the GDPR. Hence, GDPR compliance is a form of assurance that the company is more likely to follow fair privacy practices. Even though GDPR is restricted to the EU, many international companies form a common international privacy policy and follow them in the United States. As a result, even though the United States is not within the scope of GDPR, it still influences a company's privacy policies and practices in the United States.

5.1.1. Treatment
We use a control group – treatment group experimental set up to test the effect of GDPR on privacy concerns. Participants were randomly assigned to the groups. The control group was given information on a hypothetical fitness wearable and was provided with the hypothetical company's privacy policy. The given privacy policy summarized key privacy practices and data management policies. This privacy policy is adapted from a recent privacy policy of a fitness wearable company. Once the participants have read the information on the wearable and privacy policy, they were asked to complete a questionnaire that measured their perceptions of the effectiveness of privacy policy, privacy risks, privacy control, privacy concerns, and their disposition to value privacy. The scales were adapted from previous literature and is on a 7-point scale.

In the treatment group, participants were also provided with information on a hypothetical fitness wearable and privacy policy. In addition, the participants were informed that the hypothetical company is GDPR compliant and were provided with information on GDPR and its details. Once the participants have read through all the information provided, they were asked to complete the same questionnaire.
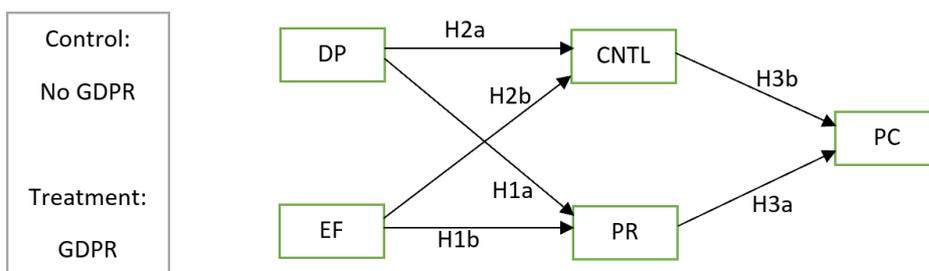

Figure 2. Research model for experiment

6. Data Analysis and Results

The data was collected from undergraduate students enrolled in a business course. The participants were of age between 18 and 25 with a mean age of 21. We obtained a total of 85 responses including 42 in control and 45 in treatment conditions. After removing responses that failed checks, a total of 70 usable responses (treatment-33 and control-37) were obtained. The demographic properties are summarized in table A1 in appendix. About 71 percentage of respondents were males and 86 percent were white. Sixty-nine percent of respondents had no previous fitness wearable device usage experience and 37 percent did not have any other smart IoT device (other than smart phones) usage experience.

6.1. Evaluating Measurement Model

We evaluated the discriminant and convergent validity of the scales by using Cronbach alpha, composite reliability, average variance extracted (AVE), loadings, and heterotrait-monotrait ratio of correlations (htmt). The items of the scales and their loadings are given in table A2 in appendix. All the items except CNTL1 and PE1 have a loading above 0.7. The Cronbach alpha, composite reliability and AVE are all above 0.8, 0.71, and 0.46 respectively. After Dropping items CNTL1 and PE1, all the items had a loading are above 0.7 and the composite reliability and AVE increased.

When all items were included in the analysis, the Cronbach alpha of PC, PR, CNTL, EF, DP, and PE were 0.90, 0.91, 0.79, 0.81, 0.85, and 0.65 respectively. After dropping the items CNTL1 and PE1, the Cronbach alpha of the variable PE increased to 0.79 (see table 2 for Cronbach alpha, composite reliability and AVE of other variables after removing CNTL1 and PE1). Similarly, including all items in analysis yielded a composite reliability of 0.90 for PC, 0.91 for PR, 0.79 for CNTL, 0.80 for EF, 0.86 for DP, and 0.71 for PE. Removing CNTL1 and PE increased the composite reliability to 0.79 for PE. The AVE for the variable CNTL increased from 0.51 to 0.57 and for PE from 0.46 to 0.66 when the items CNTL1 and PE1 were removed. The AVE for PC, PR, EF, and DP were 0.71, 0.74, 0.58, and 0.68 respectively when all items were included.

Table 2 shows that all the values in the htmt table (excluding diagonals) are below 0.9 as suggested by Henseler et al. [10]. This shows that discriminant validity is achieved. All the values in htmt were below 0.9 even when all items were included in the analysis. For further analysis, we did not add items CNTL1 and PE1. The analysis results did not change qualitatively even when all items were included.

6.2. Effect of GDPR

To test the effect of GDPR on privacy concerns (hypothesis I), we first evaluated the latent mean of privacy concerns for control and treatment group. A one-sided t-test was used to see the difference between the mean privacy concerns of the two groups. The result (table 1) suggests that the privacy concerns of treatment group is significantly lower compared to control group. This confirms our expectation that GDPR compliance by organization reduces users' privacy concerns regarding data collected by fitness wearable.

Table 1. Latent mean of privacy concerns for control and treatment group

	Control	Treatment	t	P value
PC (latent mean)	3.59	3.03	1.91	0.03**
**** significant at 5%**				

6.3. Testing the Structural Model

After establishing measurement validity, structural model was evaluated using SEM packages 'lavaan' and 'semTools' in R. Previous privacy experience, fitness wearable usage experience, and previous smart IoT device usage experience were included as control variables in the analysis. SEM path analysis were conducted for the entire data as well as separately for the control and the treatment group. The path coefficients of treatment group were not significantly different from the corresponding path coefficients of control group. We expected the average privacy concerns of treatment group to be lower than control group. However, we did not expect the relationships between variables to be different for both groups and results suggests the same. The overall SEM path analysis have signs as expected per the hypothesis (table 3). The relationship between DP and CNTL is non-negative as opposed to the hypothesis. However, the estimate is close to zero and non-significant. For the overall model, all the hypothesis except H2a and H3b are significant. The relationship between disposition to value privacy and perceived privacy control (H2a) is not significant in all three analysis – overall model, control group and treatment group.

Table 2. Properties of scales

	Heterotrait-Monotrait Ratio of Correlations (HTMT)						Cronbach alpha	Composite reliability	Variance Extracted
	PC	PR	CNTL	EF	DP	PE			
PC	1.00						0.90	0.91	0.71
PR	0.82	1.00					0.91	0.92	0.74
CNTL	0.45	0.47	1.00				0.79	0.80	0.57
EF	0.52	0.42	0.88	1.00			0.81	0.81	0.58
DP	0.73	0.62	0.26	0.29	1.00		0.85	0.86	0.68
PE	0.74	0.52	0.45	0.45	0.60	1.00	0.79	0.79	0.66

All non-diagonal elements of HTMT are below 0.90

Table 3. Results of structural model

	Estimate (standard error)	Estimate (standard error)	Estimate (standard error)	Supported
	Overall	Control	Treatment	
H1a: DP →PR	0.50**	0.76*	0.53**	Yes
	(0.15)	(0.45)	(0.17)	
H1b: EF → PR	-0.42**	-0.84**	-0.22	Partially yes
	(0.19)	(0.41)	(0.28)	
H2a: DP → CNTL	0.02	-0.55	0.09	No
	(0.11)	(0.54)	(0.11)	
H2b: EF → CNTL	0.94**	1.25**	0.99**	Yes
	(0.20)	(0.52)	(0.39)	
H3a: PR → PC	0.67*	0.52**	0.85**	Yes
	(0.13)	(0.17)	(0.19)	
H3b: CNTL → PC	-0.09	0.34	-0.67**	Partially yes
	(0.15)	(0.21)	(0.25)	

* significant at 10%
** significant at 5%

7. Discussion, Limitations, and Future Research

This study developed and empirically tested the factors that affect privacy concerns. Also, using an experimental design this study showed that GDPR can reduce privacy concerns. We use a sample of undergraduate students as participants. Since people of this age group are more familiar with technology and social media, they are less concerned with privacy compared to other age groups [13]. Consequently, our results are more conservative.

7.1. GDPR and Privacy Concerns

The results suggest that GDPR reduces users' privacy concerns. GDPR is a regulation that aims at regulating the data collection and management. It gives users with the power to control or manage the release and use of their private data. GDPR gives users an assurance on the fair and transparent management of their data. As a result, a regulation like GDPR can reduce users concerns regarding the management of their personal data and thus privacy. The treatment group were told that the organization is GDPR compliant and their average privacy concerns were significantly lower compared to control group.

7.2. Antecedents to Privacy Concerns

This study looked at the antecedents of privacy concerns like disposition to value privacy, perceived effectiveness of privacy policy, perceived privacy control, and perceived risks. Results show that users who perceive higher effectiveness of privacy policy experience higher control over their privacy. Data collection, monitoring and sharing generally leads to a perception of loss of control over data [1]. However, more information on how the data is collected, monitored and shared can help users understand how their data is disseminated. In additions, when users perceive that an organization's policies are effective and representative of their practices, users' may not experience a loss of control. Similarly, when perceived effectiveness of privacy policy is high, users perceive lower privacy risks. On the other hand, when the disposition to privacy is high, users perceive higher risks. Individuals maintain a personal boundary on information sharing that preserves their personal information [28]. An individual who is highly sensitive to privacy are likely keep their boundaries closed and when personal data is asked, they consider it as a threat to the boundary and perceive higher risks to privacy.

According to communication privacy management theory [18], privacy concerns are formed by the mental process of assessment of perceived risks and perceived controls [28]. Our results support the relationship between perceived privacy risks and privacy concerns. When perceived risks are higher, users experience more privacy concerns. However, the relationship between perceived privacy control and privacy concerns is insignificant in control group and overall data. But this relationship (CNTL → PC) is significant in the treatment group. Higher perception of privacy control is associated with lower levels of privacy concerns in the treatment group.

The relationship between disposition to value privacy and perceived privacy control is not significant in this study. One possible explanation is that the perception of control over data is possibly more dependent on the information on how data is collected and managed and how users can regulate the use and dissemination of their personal data. For instance, even if a user has lower disposition to privacy, they may perceive lower control if clear information on data management is not provided.

7.3. Contributions and Limitations of the Study

One of the key contributions of this study is establishing the causal relationship between GDPR compliance and privacy concerns using the experimental design. In general, literature on the antecedents to privacy concerns is scarce. This study attempts to fill this gap by studying the antecedents to privacy concerns in the context of wearable IoT, especially fitness wearables. Also, this study shows the relationship of perception of effectiveness of privacy policy towards privacy control and privacy risks perceptions in the context of wearable IoT devices. This study also analyses the ways by which privacy concerns can be mitigated – through privacy policies, regulations (GDPR) and by privacy controls. Even though the causal effect of only GDPR can be concluded from this study, the correlational effect of privacy policies and privacy controls on privacy concerns can be understood from this study. The causal relationship of privacy controls with privacy concerns can be found out using experimental design in future studies. Providing users with more option to control how their data is managed can increase their perception of control and reduce privacy concerns. This can be achieved by including privacy control options in the settings of the device. In future study, the level of privacy controls can be manipulated to see whether privacy controls reduce privacy concerns.

One of the limitations of this study is its generalizability. Since the study uses experimental design and the limited demographics variability of the data, results may not be generalized to a wider population. This can be addressed by using a multi-study design involving a survey study using a wider demographics and larger sample size. Another major limitation of the study is the limited sample size. Since GDPR is a regulation in EU, a better study design would be to use participants from EU for the treatment group and participants from the United States for the control group. Besides these limitations, this study explores the factors affecting privacy concerns and how it is affected by GDPR compliance.

8. Conclusion

This research analyzed how policies and regulations can reduce privacy concerns regarding the data collected by fitness wearables, which is

required to increase their adoption. Our study has implications for both academics and practitioners. Our study tries to understand the antecedents to privacy concerns like dispositions to value privacy and the effectiveness of privacy policy (a factor that can be manipulated externally). Moreover, to the best of our knowledge, this is the first study that empirically shows GDPR can reduce users' privacy concerns. Practitioners can also find the results useful in improving the marketing strategy of wearables. Since GDPR is shown to be effective in reducing privacy concerns in our study, it may be explicitly mentioned and explained in promotional materials in the US to reduce privacy concerns and increase the likelihood of adoption of the product. In summary, our study provides a preliminary understanding on the usefulness of a unified data management regulation to protect users' privacy.

9. References

[1] M. Arcand, J. Nantel, M. Arles-Dufour, and A. Vincent, "The Impact of Reading a Website's Privacy Statement on Perceived Control Over Privacy and Perceived Trust", Online Information Review., vol. 31, no. 5, pp. 661-681, 2007.

[2] N.F. Awad, and M.S. Krishnan, "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and The Willingness to be Profiled Online for Personalization", MIS Quarterly, vol. 30, no. 1, pp. 13-28, 2006.

[3] A.I. Canhoto, and S. Arp, "Exploring the Factors that Support Adoption and Sustained Use of Health and Fitness Wearables", Journal of Marketing Management, vol. 33, no. 1-2, pp. 32-60, 2017.

[4] T. Coughlan, M. Brown, R. Mortier, R.J. Houghton, M. Goulden, and G. Lawson, "Exploring Acceptance and Consequences of the Internet of Things in the Home", IEEE International Conference on Green Computing and Communications, pp. 148-155, 2012.

[5] M.J. Culnan, and P.K. Armstrong, "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation", Organization Science, vol. 10, no. 1, pp. 104-115, 1999.

[6] T. Dinev, and P. Hart, "An Extended Privacy Calculus Model for E-Commerce Transactions", Information Systems Research, 17(1), 61-80, 2006.

[7] T. Dinev, A.R. McConnell, H.J. Smith, "Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the 'APCO' Box", Information Systems Research, vol. 26, no. 4, pp. 639-655, 2015.

[8] M.S. Featherman, and P.A. Pavlou, "Predicting E-Services Adoption: A Perceived Risk Facets Perspective", International Journal of Human-Computer Studies, vol. 59, no. 4, pp. 451-474, 2003.

[9] R.D. Gopal, H. Hidaji, R.A. Patterson, E. Rolland, and D. Zhdanov, "How Much to Share with Third Parties? User Privacy Concerns and Website Dilemmas", MIS Quarterly, vol. 42, no. 1, pp. 143-163, 2018.

[10] J. Henseler, C.M. Ringle, and M. Sarstedt, "A New Criterion for Assessing Discriminant Validity in Variance-Based Structural Equation Modeling", Journal of the academy of marketing science, vol. 43, no. 1, pp. 115-135, 2015.

[11] M.M. Hossain, V.R. Prybutok, "Consumer Acceptance of RFID Technology: An Exploratory Study", IEEE Transactions on Engineering Management, vol. 55, no.2, pp. 316-328, 2008.

[12] N. Hu, P.A. Pavlou, and J. Zhang, "Can Online Reviews Reveal a Product's True Quality?: Empirical Findings and Analytical Modeling of Online Word-of-Mouth Communication", Proceedings of the 7th ACM Conference on Electronic Commerce, pp. 324-330, 2006.

[13] M. Kezer, B. Sevi, Z. Cemalcilar, L. Baruh, "Age Differences in Privacy Attitudes, Literacy and Privacy Management on Facebook", Cyberpsychology: Journal of Psychosocial Research on Cyberspace, vol. 10, no. 1, 2016.

[14] D.J. Kim, D.L. Ferrin, and H.R. Rao, "A Trust-Based Consumer Decision-Making Model in Electronic Commerce: The Role of Trust, Perceived Risk, and Their Antecedents", Decision Support Systems, 44, no.2, pp. 544-564, 2008.

[15] K. Mercer, M. Li, L. Giangregorio, C. Burns, and K. Grindrod, "Behavior Change Techniques Present in Wearable Activity Trackers: A Critical Analysis", JMIR mHealth and uHealth, vol. 4, no. 2, 2016.

[16] V.G. Motti, and K. Caine, "Users' Privacy Concerns About Wearables", International Conference on Financial Cryptography and Data Security, Springer, Berlin, Heidelberg, pp. 231-244, 2015.

[17] P.A. Pavlou, and D. Gefen, "Building effective online marketplaces with institution-based trust", Information Systems Research, vol. 15, no. 1, pp. 37-59, 2004.

[18] S.S. Petronio, Boundaries of Privacy: Dialectics of Disclosure. Albany, NY: State University of New York Press, xix, pp. 268, 2002.

[19] M. Poikela, and E Toch, "Understanding the Valuation of Location Privacy: A Crowdsourcing

Based Approach", Hawaii International Conference on System Sciences, vol. 50, pp. 1985-1994, 2002.

[20] A. Prasad, J. Sorber, T. Stablein, D. Anthony, and D. Kotz, "Understanding Sharing Preferences and Behavior for mHealth Devices", Proceedings of the 2012 ACM Workshop on Privacy in the Electronic Society, pp. 117-128, 2012.

[21] P.G. Schierz, O. Schilke, and B.W. Wirtz, "Understanding Consumer Acceptance of Mobile Payment Services: An Empirical Analysis", Electronic Commerce Research and Applications, vol. 9, no. 3, pp. 209-216, 2010.

[22] H. Sheng, F.F. Nah, and K. Siau, "An Experimental Study on Ubiquitous Commerce Adoption: Impact of Personalization and Privacy Concerns", Journal of the Association for Information Systems, vol. 9, no. 6, pp. 344-376, 2008.

[23] H.J. Smith, T. Dinev, and H. Xu, "Information Privacy Research: An Interdisciplinary Review", MIS Quarterly, 35(4), 989-1015, 2011.

[24] S. Spiekermann, "Perceived Control: Scales for Privacy in Ubiquitous Computing", Digital Privacy, Auerbach Publications, pp. 274-288, 2007.

[25] T. Spil, A. Sunyaev, S. Thiebes, and R. Van Baalen, "The Adoption of Wearables for a Healthy Lifestyle: Can Gamification Help?", Proceedings of the Hawaii International Conference on System Sciences, vol. 50, pp. 3617-3626, 2017.

[26] J. Sutanto, E. Palme, C.H. Tan, and C.W. Phang, "Addressing the Personalization-Privacy Paradox: An Empirical Assessment from Field Experiment on Smartphone Users", MIS Quarterly, vol. 37, no. 4, pp. 1141-1164, 2013.

[27] A.F. Westin, Privacy and Freedom, Athenaeum, New York, 1967.

[28] H. Xu, T. Dinev, J. Smith, and P. Hart, "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances", Journal of the Association for Information Systems, vol. 12, no. 12, pp. 798-824, 2011a.

[29] H. Xu, X.R. Luo, J.M. Carroll, and M.B. Rosson, "The Personalization Privacy Paradox: An Exploratory Study of Decision-Making Process for Location-Aware Marketing", Decision Support Systems, vol. 51, no. 1, pp. 42-52, 2011b.

[30] H. Xu, H.H. Teo, B.C. Tan, and R. Agarwal, "Research Note—Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services", Information Systems Research, vol. 23, no. 4, pp. 1342-1363, 2012.

[31] H. Xu, H.H. Teo, and B. Tan, "Predicting The Adoption of Location-Based Services: The Role of Trust and Perceived Privacy Risk", International Conference on Information Systems Proceedings, Paper 71, pp. 897-910, 2005.

Appendix

Table A1. Demographic variables

Variables	Category	Frequency	Variable	Category	Frequency
Ethnicity	White	60	Household income	< 20,000	14
	Black	2		20,000-39,999	6
	Asian	4		40,000-59,999	11
	Other	4		60,000-99,999	10
				>100,000	29
Gender	Female	20	Other smart devices	Yes	44
	Male	50		No	26
Fitness wearable owner	Yes	22	Treatment condition	Treatment	33
	No	48		Control	37
Total observations					**70**

Measures of construct and sources	Loadings (1)	Loadings (2)
Privacy Concerns (PC) [6]: I am concerned that		
PC1: the information collected by the fitness wearable device could be misused	0.90	0.90
PC2: others can find private information about me collected by fitness wearable device	0.86	0.86
PC3: collection of personal information by fitness wearable device, because of what others might do with it	0.82	0.82
PC4: collection of personal information by fitness wearable device, because it could be used in a way I did not foresee	0.79	0.79
Perceived Privacy Risks (PR) [6]: I believe that there is risk for fitness wearable device users due to the possibility that	0.85	0.85
PR1: your information could be sold to third parties	0.76	0.76
PR2: personal information collected could be misused	0.91	0.91
PR3: that personal information could be made available to unknown individuals or companies without your knowledge	0.91	0.91
PR4: personal information could be made available to government agencies		
Perceived Privacy Control (CNTL) [28]: I believe I	0.58	-
CNTL1: have control over who can get access to my personal information collected by fitness wearable device	0.70	0.73
CNTL2: have control over what personal information is released by this company	0.83	0.84
CNTL3: have control over how personal information is used by this company	0.72	0.70
CNTL4: can control my personal information collected by the fitness wearable device		
Perceived Effectiveness of Privacy Policy (EF) [28],[17]:		
EF1: I feel confident that this companies' privacy statements reflect their commitments to protect my personal information	0.76	0.76
EF2: With their privacy statements, I believe that my personal information will be kept private and confidential by this companies	0.81	0.81
EF3: I believe that these companies' privacy statements are an effective way to demonstrate their commitments to privacy	0.71	0.71
Disposition to Value Privacy (DP) [28]:		
DP1: Compared to others, I am more sensitive about the way companies handle my personal information	0.87	0.87
DP2: To me, it is the most important thing to keep my information privacy	0.71	0.71
DP3: Compared to others, I tend to be more concerned about threats to my information privacy	0.87	0.87
Previous Privacy Experience (PE) [28],[31]: How often have you		
PE1: personally experienced incidents whereby your personal information was used by someone without your authorization?	0.38	-
PE2: personally been the victim of what you felt was an improper invasion of privacy?	0.73	0.74
PE3: heard or read during the last year about the use and potential misuse of consumer's personal information without consumer's authorization by some service provider?	0.88	0.88

*Items CNTL1 and PE1 are not included in loadings (2) column