The New Wave of Privacy Concerns in the Wearable Devices Era

Nasim Talebi, Cory Hallam, Gianluca Zanella
University of Texas at San Antonio, San Antonio, TX - USA

Abstract--**The pervasiveness of mobile devices such as smart phones, apps, remote monitoring devices, and wearable sensors is enabling growth of Patient Generated Health Data (PGHD) through which people are capturing their vital signs outside the clinical settings. Tracking fitness, helping with personal health issues, tracking diet and nutrition, tracking sleeping conditions, along with managing stress and mental health are touted as potential benefits of using wearable device services. However, following the trend of growth in electronic data breaches over the last few years, information privacy intrusion has become a major potential threat associated with collecting, tracking, storing, and sharing personal information. Drawing upon literature concerning privacy conceptualization, operationalization, and perception, we aim to explain the antecedents and outcomes of privacy concerns in the context of wearables to gain more insight about users' decisions on disclosing their personal health information. We may be on the crux of a golden age for personalized collaborative care through PGHD, yet we need to consider if we are doing so by trading-off privacy.**

I. INTRODUCTION

2014 was addressed by many experts as the "Year of the Wearable," reflecting the revolution of new wearable products such as smart glasses, smart watches, hearables, fitness and health trackers or even smart jewelry and smart fashion [21]. In addition, the number of connected wearable devices worldwide is expected to increase from 109 million in 2014 to 578 million by 2019 [22].

Wearable devices are gadgets that are rapidly multiplying and can be strapped onto or even embedded in human bodies. The most familiar gadgets are fitness trackers and smart watches monitoring health conditions and providing the users/patients with complete access to online data services. But the potential of wearable devices depends significantly on the large amounts of data they generate and access [5]. A key issue concerning wearable devices arises from the amount of personal data they gather from their users. In a report written for Nature, [5] identified that "when the Pew Research Center, an independent fact-gathering organization in Washington DC, canvassed 1,600 experts in 2014 about the future of the Internet, many expressed substantial concerns about privacy and people's abilities to control their own lives".

Since technology introduces greater uncertainty about who has access to information and how it is used, greater attention has been placed on the terms of privacy assurance statements and privacy customization features associated with wearable devices. However, examination of website policy disclosures have shown that privacy policies and adherence to them vary across industries [14, 34]. Generally, information privacy is a growing concern [47, 55] creating fears for storing and sharing personal information. Yet, even with greater privacy concerns in the general public, especially in healthcare, using wearable devices that potentially generate data is increasing very fast. From this observation we posit that either users' behaviors reflect lower privacy concerns, or other factors diminish privacy concerns [15]. The objective of our research is to address this paradox by attempting to understand the other factors involved in this behavioral process.

Reference [47] categorized privacy research into eight main groups, namely employment, biographical, consumer, medical, financial, behavioral, general, and public information. Prior literature suggests that individuals are more concerned about their health information compared to any other types of personal information [20, 27]. Reference [3] suggests, "There is little else that is as consequential to an individual as his or her health information". Considering the interest and growth in this area, we are attempting to develop a mechanism to answer two specific research questions: (1) what is the role of privacy assurance mechanisms in alleviating patients' privacy concerns? And (2) what are the roles of privacy concerns, perceived ownership of personal information and subjective norms in patients' self-disclosure behavior?

In the following sections, we develop a theoretical model that explores privacy behavior, including antecedents related to the disclosure of personal health information in the context of wearable device and Patient Generated Health Data (PGHD). The subsequent sections describe data collection procedures, survey instrument validation, and model testing using Partial Least Square Path Modeling (PLSPM) analysis. We then discuss the contributions of this paper followed by the limitation and future directions. The last part provides a summarizing conclusion.

II. RESEARCH BACKGROUND

As technology becomes further embedded in our lives, and daily activities, those who want to participate are required to disclose even more personalized data. Self-disclosure refers to "what individuals voluntarily and intentionally reveal about themselves to others – including thoughts, feelings and experiences" [43]. Disclosing personal information makes wearable users vulnerable to various types of privacy risks. However, people keep using wearable devices and disclosing their information through social networks and infomediaries. This contrast of information privacy concern and actual behavior has been called the privacy paradox [9, 39]. This phenomenon has been studied

from different theoretical lenses such as privacy calculus theory, social theory, cognitive biases and heuristics in decision-making, and decision-making under bounded rationality and information asymmetry conditions [28]. Privacy calculus aassumes that individuals make decisions between the expected loss of privacy and the potential gain of disclosure, and the final behavior is determined by the outcome of this trade-off [15, 26, 55]. Social theory is based on the extent to which social networking has penetrated into our lives such that people feel they have to disclose information on them in spite of their privacy concerns [8].

In contrast to privacy calculus, cognitive biases and heuristics in decision-making believe that human decision-making is affected by cognitive biases and heuristics [2]. Bounded rationality perspective lies on the assumption of cognitive limitations in human decision making arising from information asymmetry between consumer and providers of information [1]. Hence, due to the complexity and the influence of uncertainty and ambiguity, providing more privacy information may not be always beneficial to the individual as it may lead to more cognitive costs, heuristics, and biases. Considering all those theoretical perspective, we cannot understand this paradox correctly without taking factors such as privacy assurance, social influence or even the feeling of ownership for the data being generated by users/patients.

In summary, prior research in information privacy, wearable device, and healthcare information systems have all mentioned the need for further investigation on users' privacy concerns and their self-disclosing behavior. Considering users' concern, different web sites and app developers are actively taking the responsibility of ensuring users about the privacy of their data offering privacy assurance mechanisms. But, are they really helpful in decreasing concerns and encouraging people to do self-disclosure? Therefore, in this study, we will focus on the privacy assurance mechanisms to understand whether they can be influential or not. In addition, since privacy is a complex decision problem resulting in attitudes and behaviors that differ significantly from one individual to another, we are interested in figuring out if other people's approach have an effect on our decision to disclose or not. Therefore, we are going to elaborate more on each of those mentioned dimensions (privacy assurance mechanisms, privacy concern, perceived ownership, social norms, and self-discloser) in the following section.

III. RESEARCH MODEL AND HYPOTHESES

A. Privacy concern

Privacy concern is defined as "an individuals' concern about the threat to their information privacy when submitting their personal information on the Internet" [6, 48]. Previous studies show conflicting results about the effect of privacy concerns on self-disclosure. Although a negative relationship between privacy concern and the willingness to self-disclose has been identified in the context of e-commerce [15], as well as in the context of Social Networking Sites (SNS) [e.g. 48, 36, 37], [38] found that there is no direct significant relationship between these two. However, they showed that protection motivation fully mediates the effect of privacy concern on self-disclosure.

Since higher privacy concern reflects perceived vulnerability and hence reduce patients' willingness to disclose private information, users who are more concerned about their privacy disclose less comparing to people who are privacy apathy or the ones that have less privacy concerns. As such, we propose the following hypothesis:

H1: There is a negative relationship between privacy concern and self-disclosure in using wearable devices.

B. Perceived ownership

Perceived ownership is the feeling of possession and power [18] about one's information. The effect of perceived ownership has been examined in the previous studies [e.g. 46, 4, 52]. In a recent study to understand situational factors such as privacy apathy, perceived ownership, perceived fairness, and risks and benefits affecting information disclosure in social commerce environment, [46] found a contrary result to what they expected about the effect of perceived ownership on information disclosure. They expected that perceived ownership would negatively affect information disclosure during a social commerce transaction. However, their results did not show any significant relationship between perceived ownership and information disclosure.

One of the reasons proposed was that users may believe that their information is already out there for companies to track, so there is no particular feeling of data ownership at all. Nevertheless, the assumption of lack of information ownership in online shopping and purchases [46, 13] is not true in the context of PGHD which is being done completely deliberately. Thus, we believe that the more people have the feeling of possession or ownership of their information, the less likely they are willing to share and disclose them. Therefore, we hypothesized that:

H2: There is a negative relationship between perceived ownership and self-disclosure in using wearable devices.

C. Subjective norm

Subjective norm or social influence refers to the extent to which user's decision-making is influenced by others' perceptions [49, 53]. The positive effect of social influence on the use and acceptance of technology such as e-Government services [25], and telemedicine technology [12] have been demonstrated. However, there are some inconsistencies regarding this relationship in the context of healthcare [19, 32, 33, 48, 49].

In their study of adoption of mobile health services, [48] found that there is a positive relationship between subjective norms and the use of mobile health services. In addition, [19] found that among all factors that affect an individual's intention to adopt healthcare wearable devices, social influence and perceived privacy risk are the most significant

predictors. They emphasized that consumers using healthcare wearable devices are more affected by others ' behaviors and privacy concerns when it comes to manage their health conditions. However, previous studies regarding health technology acceptance and use by professionals have shown that social influence does not play an important role [e.g. 12] because most professionals are certain about their decisions and are not worried about others' opinions.

Reference [33] developed a framework to investigate user acceptance and use of biometrics and found that the subjective norm does not have any impact on consumer intentions to accept and use a biometric system. They concluded that it may mean that social influence is not as much relevant for this type of technology as other variables such as trust in technology, concern for data privacy, perceived risks and innovativeness. Now, due to the growing frequency of using wearable devices and different mobile apps along with many benefits arising from using them, people are encouraging each other to do the same. Therefore, we hypothesize that:

H3: There is a positive relationship between subjective norms and self-disclosure in using wearable devices.

D. Privacy assurance mechanisms

Privacy assurance refers to "mechanisms that directly or indirectly provide customers with assurances and guarantees that their private information will be protected and kept private by the website" [6, 29]. It has been found that privacy assurance mechanisms are among the most important website features for creating a trusted online environment [32] which can be extended to the mobile apps offered by different developers along with wearable devices. Having privacy assurance mechanisms in mind, wearable device users can protect themselves against threats of information disclosure [6, 38]. These mechanisms can be categorized into two main categories, namely privacy assurance statements and privacy customization features.

Privacy assurance statements are communicated from app developers and wearable device designers to patients. They typically include statements about the adequacy of their protection measures [6]. Research shows that when consumers understand that organizations have collected and used their personal information without their permission, their privacy concerns get triggered [10]. However, it has been found that consumers become less concerned about their privacy when organizations ask for consumers' permission to collect and use their information [40]. Particularly, it has been found that privacy assurance statement has a negative effect on privacy concern by decreasing the susceptibility of privacy threat and increasing perceived effectiveness of assurance mechanisms [38]. Therefore, if consumers are asked for permission and develop an understanding of what is going to be done with their data, the more protection they perceive from the privacy assurance statement the less they have privacy concern. As a result, one can expect that privacy assurance mechanisms can play a vital role in decreasing consumers' privacy concerns, leading to the following hypothesis:

H4a: There is a negative relationship between privacy assurance statement and privacy concern in using wearable devices.

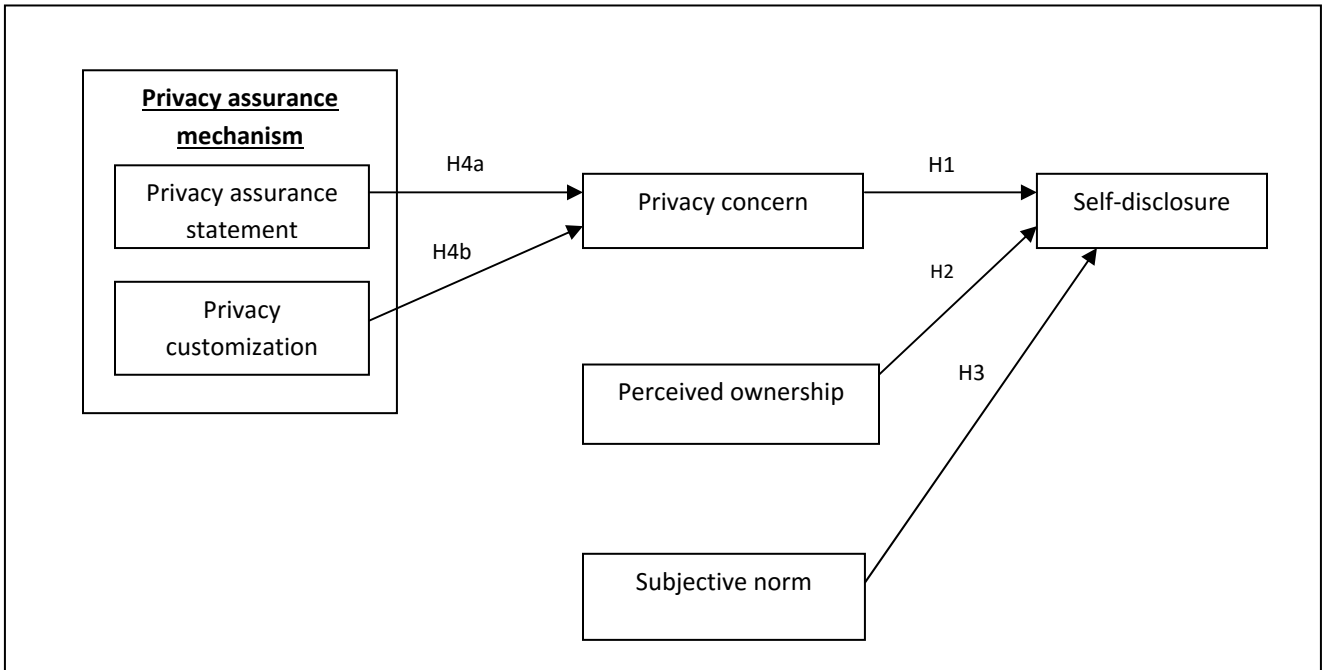

Figure 1. Research model

Privacy customization refers to consumers' efforts to use different features to change and control the flow of their information [55]. Privacy customization features have been studied in the context of Social Networking Sites (SNS) and it has been found that privacy customization features on SNSs do not have a significant influence on users' assessment of the threat because there are several different tools such as web surfing tools and cookie management tools enabling users to protect themselves against privacy threats [38]. However, when it comes to more sensitive information such as health information, individuals employ a "pre-caution" strategy in order to protect themselves from threats [30 as cited by 38]. Likewise patients using wearable devices limit the access of others to their personal health information through which they have a perceived control over their information and, as a result, feel less vulnerable towards privacy threats. Therefore, apps or programs that let users customize their privacy preferences reduce user privacy concern, leading to the following hypothesis:

H4b: There is a negative relationship between privacy customization and privacy concern in using wearable devices.

IV. RESEARCH DESIGN AND DATA COLLECTION

To study the research model depicted in Fig. 1 above, we chose an empirical study approach using a survey instrument. The research instrument was developed using Qualtrics software and the scale items were adopted from already validated measures in the literature (see table 1). To ensure the face validity, the survey items were pre-tested with two independent researchers. The data were collected using a snowball approach, starting with college students and social networks. Scale items were adopted from previous literature.

TABLE 1. SOURCE OF CONSTRUCT ITEMS

Self-disclosure	Bansal and Zahedi, 2010
Privacy concern	Xu et al., 2011
Privacy assurance statement	Xu et al., 2011
Privacy customization	Mousavizadeh and Kim, 2015
Perceived ownership	Van Dyne and Pierce, 2004
Social influence	Wu et al., 2011

265 individuals participated in our survey. The age of the respondents was between 18 and 83, with the mean age of 29. A summary of the demographic information corresponding to the subjects is presented in Table 2. Accordingly, 52% of respondents were female, and about 39% of the sample had a college degree. 43% of these participants use either wearable devices or mobile apps to track their health condition or physical activity. Therefore, in order to have a representative sample to examine the self-disclosure behavior, we included 97 completed data points to do the analysis in this exploratory study. It is worth mentioning that the data set is still growing and we expect to have more responses prior to the final presentation at the conference.

TABLE 2. DEMOGRAPHIC CHARACTERISTICS OF THE SAMPLE

Characteristics		Frequency	Ratio
Gender	Male	109	41.13%
	Female	138	52.07%
	Missing	18	6.79%
	Total	265	100%
Education	No degree	3	1.13%
	High school	15	5.66%
	Some years of college, no degree	143	53.96%
	Bachelor's degree	49	18.49%
	Master's degree	25	9.43%
	Professional degree	4	1.51%
	Doctorate	8	3.02%
	Missing	18	6.80%
	Total	265	100%
Wearable device used	Smart phone apps	62	64%
	Wireless smart band	26	26.8%
	Smart watch	9	9.20%
	Total	97	100%

V. DATA ANALYSIS AND RESULTS

To test our research model using the preliminary sample that we had, we applied Partial Least Square Path Modeling (PLSPM) [45] using R software version 3.2.3. In addition, we test for the reliability of the scale items using the same software. The reliability of each construct is assessed by analyzing the Cronbach's alpha coefficient. Values above 0.7 indicate acceptable reliability of the measurement model [41, 42]. Multicollinearity was examined using Variance Inflation Factor (VIF) test.

TABLE 3.CRONBACH ALPHA AND VIF TEST RESULTS

Construct	Cronbach's Alpha Coefficient	Variance Inflation Factor
Self-disclosure	0.64	< 1.66
Privacy concern	0.93	< 3.50
Privacy assurance statement	0.93	<4.59
Privacy customization	0.95	<4.71
Perceived ownership	0.80	< 6.46
Social influence	0.87	< 2.43

In order to assess the quality of the measurement model we examined the Cronbach's alpha, the Dillon-Goldstein's rho, and the first eigenvalue to check unidimensionality. None of them shows any problem. After assessing the quality of the outer model, inner model quality was checked using path coefficients to demonstrate the strength and significance of the relationship between constructs. Considering the regression results of each endogenous construct, we found significant positive relationship between both privacy assurance statements privacy customization and privacy concern, as well as significant positive relationship between social influence and self-disclosure and a significant negative relationship between perceived ownership and self-disclosure. Fig. 2 shows the measurement model also known as outer model [45] resulting from the PLSPM analysis on the preliminary data.

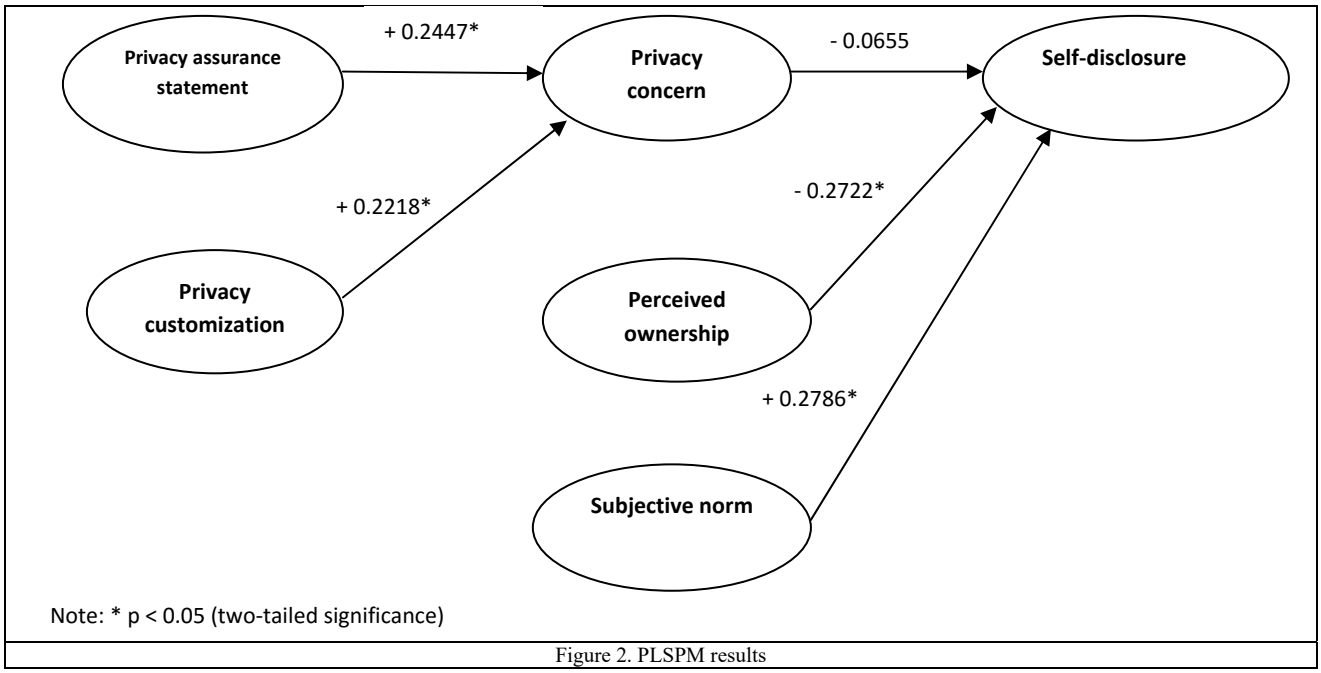

Figure 2. PLSPM results

VI. DISCUSSION

The results of this study revealed that the privacy assurance statement affects privacy concern. However, its effect was contrary to what we expected. One possible reason would be that users should perceive the privacy statement as adequate in order to feel that their privacy is protected, otherwise not only it cannot reduce the privacy concern, but also it increases users' concern regarding their privacy. Or there might be discrepancies between users' expectations and the contents of privacy assurance statement [17] that makes users to show more privacy concerns. This effect can be intensified in case of high-privacy concern individuals who are more sensitive to the adequacy and quality of the privacy statements. Therefore, it sounds that either our sample had included people with high privacy concerns (the average of 4.33 out of 7) or the privacy statements provided in health apps and wearable devices are not mature enough yet.

Moreover, results of this study showed that privacy customization features have a positive effect on users' privacy concern in the context of wearable devices. Given the strong theories supporting the relationship and strong instrument validity and fit of the data, this finding calls for further data collection. Apparently, offering privacy customization features to users make them more aware of possible threats. Therefore, it increases users perceived threat susceptibility and makes them become more concerned about the privacy of their health data being generated through wearable devices. Considering the effect of both privacy customization and privacy assurance statement, the result of this study shows that privacy assurance mechanisms increase the susceptibility of privacy threat rather than making people more confident and less concerned about their privacy. One possible reason would be similar to what [38] mentioned in the context of SNSs. They argued that there are some other uncontrolled factors threatening users' privacy such that privacy customization is not an appropriate mechanism to control them. Surprising findings related to privacy assurance mechanisms made us propose a new model through which we can test the direct effect of privacy assurance statements and privacy customization on self-disclosure, without the mediating effect of privacy concern.

Furthermore, the results showed no significant relationship between privacy concern and disclosure behavior which is in consistent with the result of previous studies on SNSs [e.g. 50, 51] and in general supports the existence of privacy paradox [28]. The privacy paradox states that online privacy concerns do not sufficiently explain online privacy behaviors on wearable device services.

In addition, the positive effect of social norms as well as the negative effect of perceived ownership on self-disclosure behavior has been found. These results show that the degree of perceived ownership for personal health information generated by using wearable devices can make changes to the degree of disclosing those personal data. Additionally, consistent with what [49] and [19] found, the positive effect of others' perceptions on self-disclosure in using wearable devices was demonstrated.

VII. CONTRIBUTION

This study makes a number of contributions. From a theoretical point of view, it reveals the process by which different privacy assurance mechanisms influence patients' privacy concerns to whether do self-disclosure or not. Most previous studies have examined privacy assurance

mechanisms in the context of e-commerce [6]. Therefore, we contribute to the current literature by applying this concept to health care, and particularly to wearable devices. In addition, to the best of our knowledge, subjective norm and perceived ownership of information have not been used in this context before. Above all, our findings can provide insights for researchers developing particular applications to gather data from patients for their research purposes that require patients to disclose their private health information. The same can be applicable for new app developers.

VIII. LIMITATION AND FUTURE RESEARCH

Like many other studies, this study has limitations. First and foremost this study is exploratory in nature, starting with a university sample and using a snowball technique to expand the dataset. Although university students are a large user of mobile applications and wearable technology, using only students as the sample might reduce the generalizability of our results. We are expanding the reach of the study through social media channels, aiming to collect data from a more diverse sample including elderlies. In addition, as it was suggested by [31], future researchers can include sub-dimensions of privacy concern such as control, collection, and awareness of privacy. Our current data set lacks multi-national cultural diversity, which can be an influential factor since different cultures may care about privacy differently [54, 7, 16]. Future studies may look at the differences in privacy concern among different cultures in the context of wearable devices. Moreover, in terms of privacy assurance mechanisms we only focused on privacy assurance statement, which is the direct mechanism of privacy assurance, and did not consider indirect features such as developers' reputation, design appeal, and perceived information quality (PIQ). Future researchers can take those indirect factors into consideration.

IX. CONCLUSION

People are using health apps and wearable devices every day in order to track their vital signs and have a healthier life, but they are going to be more vulnerable to privacy intrusion by disclosing their personal health information. It has been shown that privacy practices are highly context-sensitive [24]. As a result, we chose a very growing and significant context like healthcare, and more particularly, Patient Generated Health Data (PGHD). The purpose of this study was to understand factors affecting patients' self-disclosure behavior in generating health data. Four hypotheses were proposed through which the effect of privacy assurance mechanisms, including privacy assurance statements and privacy customization, privacy concern, subjective norm, and perceived ownership of health information were examined on self-disclosure behavior in generating health data. Our findings demonstrated that there is a positive relationship between privacy assurance mechanisms and privacy concern as well as a positive relationship between social norms and self-disclosure behavior. Additionally, a negative relationship between perceived ownership of personal health data and self-disclosure behavior was found. The results of this research has provided more insights into the disclosing of personal health information using mobile health technology and extended the literature on mobile health (m-health), information privacy, and self-disclosure.

REFERENCES

[1] Acquisti A, Grossklags J. Privacy and rationality in individual decision making. IEEE Secur Priv 2005;2:24–30.

[2] Acquisti A, Grossklags J. What can behavioral economics teach us about privacy. In: Acquisti A, Gritzalis S, Lambrinoudakis C, di Vimercati S, editors. Digital privacy: theory, technology, and practices. Auerbach Publications; 2007. p. 363–77.

[3] 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(3), 469-490.

[4] Anderson, C.L., Agarwal, R., 2010. Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. MIS Quarterly 34 (3), 613–643.

[5] Austen, K. (2015). The trouble with wearables. *Nature, 525*(7567), 22-24.

[6] Bansal, G., Zahedi, F., and Gefen, D. (2015). The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern. European Journal of Information Systems, 1-21. Retrieved from http://dx.doi.org/10.1057/ejis.2014.41

[7] Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. (2004). International differences in information privacy concerns: A global survey of consumers. The Information Society, 20(5), 313-324.

[8] Blank G, Bolsover G, Dubois E. A new privacy paradox. 2014. Working Paper, University of Oxford, Global Cyber Security Capacity Centre.

[9] Brown, B., "Studying the Internet experience". *HP LABORATORIES TECHNICAL REPORT HPL*. vol. (49), 2001.

[10] Cespedes, F. V., & Smith, H. J. (1993). Database marketing: New rules for policy and practice.Sloan Management Review, 34(4), 7.

[11] Chau, P. Y. K., & Hu, P. J. H. (2002). Investigating healthcare professionals' decisions to accept telemedicine technology: An empirical test of competing theories. Information and Management, 39(4), 297–311.

[12] Chau, P.Y., and Hu, P.J.H. "Information Technology Acceptance by Individual Professionals: A Model Comparison Approach*," Decision Sciences, Vol. 32, No. 4: 699-719, 2001

[13] Clarke, R., 1999. Internet privacy concerns confirm the case for intervention. Communications of the ACM 42 (2), 60–67.

[14] Culnan, M. J. 2000. Protecting privacy online: Is self-regulation working? J. Public Policy Marketing 19 20–29.

[15] Dinev, T., & Hart, P. (2006). An extended privacy calculus model for E-commerce transactions. *Information Systems Research, 17*(1), 61-80. doi:10.1287/isre.1060.0080

[16] Dinev, T., Bellotto, M., Hart, P., Russo, V., & Serra, I. (2006). Internet users' privacy concerns and beliefs about government surveillance: an exploratory study of differences between Italy and the United States. Journal of Global Information Management (JGIM), 14(4), 57-93.

[17] EARP JB, ANTÓN AI, AIMAN-SMITH L and STUFFLEBEAM WH (2005) Examining internet privacy policies within the context of user privacy values. IEEE Transactions on Engineering Management 52(2), 227–237

[18] Furby, L., 1978. Possession in humans: an exploratory study of its meaning and cmotivation. Social Behavior and Personality 6 (1), 49–65.

[19] Gao, Y., Li, H., & Luo, Y. (2015). An empirical study of wearable technology acceptance in healthcare. Industrial Management & Data Systems,115(9), 1704-1723. doi:10.1108/IMDS-03-2015-0087

[20] Gostin, L. O., & Nass, S. (2009). Reforming the HIPAA privacy rule: Safeguarding privacy and promoting research. Jama,301(13), 1373.

[21] Heng Xu, Hock-Hai Teo, Bernard C. Y. Tan, Ritu Agarwal, (2012) 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 23(4):1342-1363. http://dx.doi.org/10.1287/isre.1120.0416

[22] http://www.statista.com/statistics/487291/global-connected-wearable-devices/

[23] http://www.statista.com/topics/1556/wearable-technology/

[24] Hull, G. (2014). Successful failure: what Foucault can teach us about privacy self-management in a world of Facebook and big data. *Ethics and Information Technology*, 1-13.

[25] Hung, S., Chang, C., & Yu, T. (2006). Determinants of user acceptance of the e-government services: The case of online tax filing and payment system. Government Information Quarterly, 23(1), 97-122. doi:10.1016/j.giq.2005.11.005

[26] Jiang Z, Heng CS, Choi BC. Research note: privacy concerns and privacy-protective behavior in synchronous online social interactions. Inform Syst Res 2013;24(3):579–95.

[27] Kam, L. E., & Chismar, W. G. (2005;2006;). Online self-disclosure: Model for the use of internet-based technologies in collecting sensitive health information. International Journal of Healthcare Technology and Management, 7(3-4), 218-232. doi:10.1504/IJHTM.2006.008433

[28] Kokolakis, S. (2015). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*.

[29] LOWRY PB, MOODY G, VANCE A, JENSEN M, JENKINS J and WELLS T (2012) Using an elaboration likelihood approach to better understand the persuasiveness of website privacy assurance cues for online consumers. Journal of the American Society for Information Science and Technology 63(4), 755–776.

[30] Maddux, J.E., and Rogers, R.W. 1983. "Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change," Journal of experimental social psychology (19:5), pp 469-479.

[31] Malhotra, N.K., Kim, S.S., and Agarwal, J. (2004). Internet Users' Information Privacy Concerns (Iuipc): The Construct, the Scale, and a Causal Model. Information Systems Research 15(4), 336-355.

[32] Milne, G.R., and Culnan, M.J. 2004. "Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices," Journal of Interactive Marketing (18:3), pp 15-29.

[33] Miltgen, C. L., Popovic, A., & Oliveira, T. (2013). Determinants of end-user acceptance of biometrics: Integrating the "big 3" of technology acceptance with privacy context. Decision Support Systems, 56, 103-114. doi:10.1016/j.dss.2013.05.010

[34] Miyazaki, A. D., A. Fernandez. 2000. Internet privacy and security: An examination of online retailer disclosures. J. Public Policy Marketing 19(1) 54–63.

[35] Mohamed, N., & Ahmad, I. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. Computers in Human Behavior, 28(6), 2366–2375.

[36] Mohamed, N., & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. Computers in Human Behavior, 28(6), 2366 – 2375. doi:10.1016/j. chb.2012.07.008

[37] Moscardelli, D. M., & Divine, R. (2007). Adolescents' concern for privacy when using the Internet: An empirical analysis predictors and relationships with privacy protecting behaviors. Family and Consumer Sciences Research Journal, 35(3), 232–252.

[38] Mousavizadeh, M., and Kim, D. J. "A study of the effect of privacy assurance mechanisms on self-disclosure in social networking sites from the view of protection motivation theory," ICIS 2015 Proceedings

[39] Norberg, P.A., D.R. Horne, and D.A. Horne, "The privacy paradox: Personal information disclosure intentions versus behaviors". *Journal of Consumer Affairs*. vol. **41**(1): pp. 100-126, 2007.

[40] Nowak, G. J., & Phelps, J. (1995). Direct marketing and the use of individual-level consumer information: Determining how and when "privacy" matters. Journal of Direct Marketing, 9(3), 46-60. doi:10.1002/dir.4000090307

[41] Nunnally, C., and Bernstein, H., 1978 "Psychometric theory," New York: McGraw-Hill.

[42] Nunnally, J.C., Bernstein, I.H., and Berge, J.M.t., 1967. Psychometric theory McGraw-Hill New York. Ofcom 2014."Ofcom Technology Tracker."

[43] Posey, C., Lowry, P.B., Roberts, T.L., and Ellis, T.S. 2010. "Proposing the online community self-disclosure model: the case of working professionals in France and the UK who use online communities," European Journal of Information Systems (19:2), pp 181-195.

[44] S.-Y. Hung, C.-M. Chang, T.-J. Yu, Determinants of user acceptance of the e-Government services: the case of online tax filing and payment system, Government Information Quarterly 23 (1) (2006) 97–122.

[45] Sanchez, G., "Understanding partial least squares path modeling with r". Academic Paper Universitat Politècnica de Catalunya. vol., 2009.

[46] Sharma, S., & Crossler, R. E. (2014). Disclosing too much? Situational factors affecting information disclosure in social commerce environment. Electronic Commerce Research and Applications, 13(5), 305. doi:10.1016/j.elerap.2014.06.007

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

[48] Son, J. Y., & Kim, S. S. (2008). Internet users' information privacy-protective responses: A taxonomy and a nomological model. MIS Quarterly, 32(3), 503–529.

[49] Sun, Y., Wang, N., Guo, X. and Peng, Z. (2013), "Understanding the acceptance of mobile health services: a comparison and integration of alternative models", Journal of Electronic Commerce Research, Vol. 14 No. 2, pp. 183-200.

[50] Taddicken M. The 'privacy paradox' in the social web: the impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. J Comput-Med Commun 2014;19(2):248–73.

[51] Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. Bulletin of Science, Technology & Society, 28(1), 20 – 36. doi:10.1177/0270467607311484

[52] Van Dyne, L., Pierce, J.L., 2004. Psychological ownership and feelings of possession: three field studies predicting employee attitudes and organizational citizenship behavior

[53] Venkatesh, V., Morris, M.G., Davis, G.B. and Davis, F.D. (2003), "User acceptance of information technology: toward a unified view", MIS Quarterly, Vol. 27 No. 3, pp. 425-478.

[54] Wu, K.-W., Huang, S.Y., Yen, D.C., and Popova, I. 2012. "The effect of online privacy policy on consumer privacy concern and trust," Computers in human behavior (28:3), pp 889-897.

[55] Xu, H., Dinev, T., Smith, J., and Hart, P. 2011. "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances." Journal of the Association for Information Systems (12:12), pp 798-824.

[56] Yiwen Gao He Li Yan Luo , (2015),"An empirical study of wearable technology acceptance in healthcare", Industrial Management & Data Systems, Vol. 115 Iss 9 pp. 1704 – 1723