21 The Impact Of Privacy On Wearable Computing Adoption

V. Yfantis[1],
Dpt. of Computer Science, Electrical and Space Engineering, Luleå University of Technology, Luleå, Sweden,
E-mail: Byfantis@yahoo.com

D. Tseles
Dpt. of Automation Engineering, Piraeus University of Applied Sciences, Aigaleo, Greece,
E-mail: dtsel@teipir.gr

21.1 Abstract

There are several factors that may influence the user's intention to adopt wearable computing, including technical and non technical factors. The scope of the current framework is to build a model for the measurement of the impact of the privacy factor towards the intention of the user to adopt the wearable computing.

21.2 Background

Wearable computing as an extension of mobile computing may overlap the market share of the mobile computing, such as smartphones; however, this fact depends on the behavior of the user towards the adoption and use of both wearable computing devices and «classic» mobile computing devices. The adoption of the wearable computing devices by the users depend on several factors that may affect his/her decision to adopt the wearable computing technology. MarketResearch.com which is a website that collects business intelligence reports from around the world, mentions a few of the most influential adoption factors (Staff, 2014). Security is also an important influencing factor, because a wearable computing device that has been hacked, may grant access to the personal data of the user from non authorized persons. The worst case scenario is the unauthorized person who gains access to the hardware may cause a physical damage to the user by increasing the temperature of the device or even making it to explode! The current research framework about the impact of security on the adoption of wearable computing is limited or even non existing.
An initial search on engines such as Google Scholar or Scopus offers limited results about the impact of security in general, on specific wearable health caring devices. Krupp and other researchers explored in 2014 the subject of security and privacy with the Google Glasses (Krupp, Schröder, & Simkin, 2014). Motti and Caine in 2015 researched the users' privacy concerns about wearable devices by conducting a qualitative content analysis of online comments regarding privacy concerns of wearable device users (Motti & Caine, 2015). The comments included concerns of criminal abuse, facial recognition, access control, speech disclosure and visual occlusion. Chan, Halevi and Memon, explored the user authentication on Google glass (Chan, Halevi, & Memon, 2015). They are referring to the vulnerability of several authentication mechanisms such as the audio passphrase to unlock the Google Glass. On this occasion, the problem is that the eavesdropping attack method is an obvious way for the hacker to find the password. Kirkham and Greenhalgh research the

risk of privacy on wearable computing for autism (Kirkham & Greenhalgh, 2015). An important risk is when the wearable devices collect audio recordings and then these data become accidentally available to the public.
The importance of security on the wearable computing as it is stated by the previous scholars and the underestimated factor of privacy on the adoption of the wearable computing, are several among the reasons that motivate me to explore the impact of security on the wearable computing adoption. By taking into account all this information, I define as a research question: *What is the impact of privacy on the adoption of the wearable computing?*

21.3 Reading The Literature

The research question of this academic effort is leading the literature review and the best way to deal with this, is to analyze each concept of the research question and then synthesize the knowledge towards answering the research question.
Mario Silic and Andrea Back in 2014 conducted a literature review about the information security research and its themes (Silic & Back, 2014). The two scholars identified thirteen research themes by using the information systems as a general application sector. The first concept of my research question is privacy which is part of the information security research area, so among all the security research themes, I am going to focus mainly on privacy. Mason states that privacy is one of the most important ethical issues of the information age (Mason, 1986) and the same argument is supported by Smith and other scholars who revise the information age and defining it as a networked society (Smith, Papadaki, et al, 2013). Privacy is the security area that is related to the relationship between technology and the access to personal data. Privacy is a widely explored subject at the information security research area.
The “wearable computing adoption” part of the research question is divided into the “wearable computing” that was explored in the background part of this work and the “adoption” part that refers to the information system adoption. Information system adoption is a multi disciplined research area; however this work is focusing only on the technology element of the information systems because it considers wearable computing as technology. The technology adoption is explored by several scholars as technology acceptance. According to Khasawneh, “technology adoption is the first use or acceptance of a new technology or new product” (Khasawneh, 2008). There are several technology acceptance models, however the most popular according to Gangwar (Gangwar, Date, & Raoot, 2014) and Oliveira (Oliveira & Martins, 2010), are:
Technology Acceptance Model (Davis, 1989), Theory Of Reasoned Action (Fishbein & Ajzen, 1975), Theory Of Planned Behavior (Ajzen, 1991), Technology Organization Environment (Tornatzky & Fleischer, 1990), Unified Theory Of Acceptance and Use of Technology (UTAUT) (Venkatesh, Morris, Davis, & Davis, 2003), Diffusion Of Innovations (Rogers, 1995).
After the analysis of the research question, the next step is to perform the research at several sources of information in order to find the knowledge gap and build the research model. The search for the literature is implemented by searching at several online databases. I performed research on electronic databases such as Scopus, Web of Science and Google Scholar. I decided to use a keyword strategy with the keywords "wearable computing" and each name of the six most popular adoption models that were mentioned previously. I performed 6 times the research, based on the six information system adoption models and then ended in 9 research papers.

According to Webster and Watson (Webster & Watson, 2002) a literature review is a concept centric process and the first step is to group our results in a concept matrix which summarizes the findings of the literature review. Specifically, the concept matrix table shows the articles that feature one or more of the six adoption theories in order to explore wearable computing adoption.

Articles	**Concepts**					
	Technology Acceptance Model	Theory Of Reasoned Action	Theory Of Planned Behavior	Technology Organization Environment	Unified Theory Of Acceptance and Use of Technology	Diffusion Of Innovations
(Kim & Shin, 2014)	X					
(Carter, 2008)	X					
(Buenaflor & Kim, 2012)	X					
(Buenaflor & Kim, 2012)	X					X
(Grabowski, 2015)	X					
(Li, Wu, Gao, & Shi, 2016)	X		X			X
(Heetae, Jieun, Hangjung, & Munkee, 2016)	X					
(Trelease, 2006)						X
(Cecchinato, Cox, & Bird, 2015)						X

Table 1 **Concept matrix**

The summarization of the concept matrix results, leads to the building of the concept centric approach of the literature review analysis (Webster & Watson, 2002) which is the second step of the literature review. The first step showed that there are 9 articles which discuss the wearable device adoption based on the six adoption models. The second step is to match those results with the privacy concept, so as to detect what has been written regarding the role of privacy on the wearable computing adoption.

Only two out of the nine papers, discuss the impact of privacy on the wearable computing adoption and those two papers use the TAM model as the research model. The paper of Buneaflor & Kim reveals that people, who use wearable devices, try to hide their personal information from the device due to the fear of unauthorized access to their data. For instance, they try to not show emotion when they wear devices that capture the emotion. Li and other scholars found that perceived privacy negatively affects the adoption of using wearable healthcare devices. So, what we know about the impact of privacy on the wearable computing is very limited. Based on the literature review method and the time of searching the databases, the results reveal that there is a knowledge gap of detecting the impact of privacy on the wearable computing adoption. I only have 2 records; however two records are

not enough to generalize knowledge about the research question. The limited knowledge that I found through the literature review about the wearable computing adoption and privacy, defines an interesting knowledge gap that encouraged me to continue my research.

21.4 Research Methodology

According to the literature review findings, the most popular models for the wearable computing adoption are: Technology Acceptance Model (Davis, 1989) and Diffusion Of Innovations (Rogers, 1995). However, both papers that discuss privacy mainly use TAM as a research model. I am choosing TAM as my research model because it is mainly used to explore the impact of privacy on wearable computing adoption.
Technology Acceptance Model is an information systems theory that estimates how the technology users are going to accept the technology. Davis (1989) argues that there are two factors that influence the user's attitude towards using a technology. Perceived usefulness is "the degree to which a person believes that using a particular system would enhance his or her job performance"(Davis, 1989). The other factor is Perceived ease of use and it is defined as "the degree to which a person believes that using a particular system would be free from effort"(Davis, 1989).
However, I am willing to use a different version of TAM. My version derives of the supported TAM constructs that have a direct impact on the intention to use, according to the literature review, the first version of TAM and the construct of privacy. "Intention to use" is a construct that leads in the actual use of the device. I am assuming that the constructs that have a direct relationship with the intention to use, are the factors that strongly influence the wearable computing adoption. Based on the literature review, next table shows the supported TAM hypotheses that are featured in all the empirical papers that I found.

TAM Scholars	Supported Hypotheses
(Kim & Shin, 2014)	**AT → IU (Attitude → Intension to use)** **CT → IU (Cost → Intension to use)**
(Davis, 1989)	**PU → IU (Perceived Usefulness → Intension to use)**
(Heetae, Jieun, Hangjung, & Munkee, 2016)	**PV → IU (Perceived Value → Intension to use)**

Table 2 ***Supported TAM hypotheses***

By taking into account the new information, I form the hypotheses that will be tested in the research model:
H1: Perceived value has a positive effect on behavioral intention to use
H2: Perceived usefulness has a positive effect on behavioral intention to use
H3: Attitude towards using has a positive effect on behavioral intention to use
H4: Perceived privacy has a positive effect on behavioral intention to use
H5: Cost has a positive effect on behavioral intention to use

21.5 Conclusions

The current research effort was designed in order to answer the main research question and achieve the research goals. By taking into account the wearable computing adoption as a rationale, I followed a scientific methodology by reviewing the existing literature and building

a research model for testing. My research question was about the impact of privacy on the adoption of the wearable computing.
The big question is what is next? How can we improve the privacy measures in order to encourage more people to adopt the wearable devices? A sociotechnical approach based on the privacy characteristics could be the answer to the problem. I would extend my research by defining a new research question about the impact of social and technical privacy on the wearable computing adoption. As social privacy, I consider the personal information that is relevant to the social status of the user (Gender, age, etc.). As technical privacy, I consider the personal technical information of the user (Log files, smartphone synchronization, etc.). Probably I would use a hybrid research methodology of experiment for the technical privacy and survey for the social privacy. My results would be a comparison between the two research methods and this research would probably reveal useful details for both marketers and technical designers of the wearable devices.

21.6 References

[1] Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes,* , 179-211.

[2] Al-Fedaghi, S. (2012). Perceived privacy. *Proceedings of the 9th International Conference on Information Technology, ITNG 2012* (pp. 355-360). Las Vegas: IEEE.

[3] Awad, N., & Krishnan, M. (2006). The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization. *MIS Quarterly* , 13-28.

[4] Barker, K. (2014). The gap between real and perceived security risks. *Computer Fraud and Security* , 5-8.

[5] Barth, A., Jackson, C., & Mitchell, J. (2009). Securing frame communication in browsers. *Communications of the ACM* , 83-91.

[6] Brown, P., Bovey, J., & Chen, X. (1997). Context-aware applications: from the laboratory to the marketplace. *IEEE Personal Communications* , 58-64.

[7] Buenaflor, C., & Kim, H. (2013). Six Human Factors to Acceptability of Wearable Computers. *International Journal of Multimedia and Ubiquitious Engineering* .

[8] Buenaflor, C., & Kim, H. (2012). Wearable Computers in Human Perspective: The Decision Process of Innovation Acceptance with User Issues and Concerns. *International Journal of Emerging Technology and Advanced Engineering* .

[9] Carter, E. (2008). Marketing "smart" medical innovation: Physicians' attitudes and intentions . *International Journal of Pharmaceutical and Healthcare Marketing* , 307-320.

[10] Cecchinato, M., Cox, A., & Bird, J. (2015). Smartwatches: the Good, the Bad and the Ugly? *CHI EA '15: Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems* (pp. 2133-2138). New York: Association for Computing Machinery (ACM).

[11] Chan, P., Halevi, T., & Memon, N. (2015). Glass OTP: Secure and convenient user authentication on google glass. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 8976, pp. 298-308. , Glass OTP: Secure and convenient user authentication on google glass, (2015) Lecture Notes in Comput* , 298-308.

[12] Cheng, L., Li, ,. Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: an integrated model based on social control and deterrence theory. *Computers and Security* , 447-459.

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

[14] Davis, F. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly* , 319-340.

[15] Dey, A., Abowd, G., & Wood, A. (1998). CyberDesk: A Framework for Providing Self-Integrating Context-Aware Services. *Knowledge Based Systems* , 3-13.

[16] Dey, A., Abowd, G., Brown, P., Davies, N., Smith, M., & Steggles, P. (1999). Towards a Better Understanding of Context and Context-Awareness. *HUC '99 Proceedings of the 1st international symposium on Handheld and Ubiquitous Computing* (pp. 304-307). London: Springer.

[17] Dodds, W., Monroe, K., & Grewal, D. (1991). Effects of price, brand and store information on buyer's product evaluations. *Journal of Marketing Research* , 307 - 319.

[18] Dongjin, K., Jeongoh, M., Seong-je, C., Jongmoo, C., Minkyu, P., Sangchul, H., et al. (2014). A birthmark-based method for intellectual software asset management. *Proceedings of the 8th International Conference on Ubiquitous Information Management and Communication.* New York: ACM.
[19] F. Mouton, L., Leenen, M., Malan, M., & Venter, ,. H. (2014). Towards an ontological model defining the social engineering domain. *11th Human Choice andcomputers International Conference* (pp. 266 - 279). Turku: Springer.
[20] Fishbein, M., & Ajzen, I. (1975). *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research.* Reading: Addison-Wesley.
[21] Gangwar, H., Date, H., & Raoot, A. (2014). Review on IT adoption: insights from recent technologies. *Journal of Enterprise Information Management* , 488 - 502.
[22] Gibbs, M. (2008). Privacy. In M. Gibbs. Pearson.
[23] Gibson, G. (1996). An introduction to seismology. *Information Management and Computer Security* , 20-25.
[24] Gou, R., & Lu, ,. T. (2013). Research on Security Management Plan for Enterprise Information Systems. *Applied Mechanics and Materials* , 2560-2563.
[25] Grabowski, M. (2015). Research on Wearable, Immersive Augmented Reality (WIAR) Adoption in Maritime Navigation. *Journal of Navigation* , 453-464.
[26] He, L., Jing, W., Yiwen, G., & Yao, S. (2016). Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective. *International Journal of Medical Informatics* , 8-17.
[27] Heetae, Y., Jieun, Y., Hangjung, Z., & Munkee, C. (2016). User acceptance of wearable devices: An extended perspective of perceived value. *Telematics and Informatics* , 256–269.
[28] Herath, T., & Rao, H. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems* , 106-125.
[29] Hirschheim, R., & Klein, H. (1989). Four paradigms of information systems development. *Communications of the ACM* , 1199-1216.
[30] Intelligence, B. (2015, May 21). *THE WEARABLES REPORT: Growth trends, consumer attitudes, and why smartwatches will dominate*. Retrieved June 1, 2016, from Business Insider: http://www.businessinsider.com/the-wearable-computing-market-report-2014-10
[31] Interior, M. o. (2010, August 11). *Kallikratis Law.* Retrieved May 18, 2016, from The Central Union of Municipalities and Communities of Greece: http://www.kedke.gr/uploads2010/FEKB129211082010_kallikratis.pdf
[32] Kang, J. (1998). Information privacy in cyberspace transactions. *Stanford Law Review* , 1193-1294.
[33] Khasawneh, A. (2008). Concepts and measurements of innovativeness: the case of information and communication technologies. *International Journal of Arab Culture, Management and Sustainable Development* , 23-33.
[34] Kim, K., & Shin, D. (2014). An acceptance model for smart watches: Implications for the adoption of future wearable technology. *Internet Research* , 527 - 541.
[35] Kirkham, R., & Greenhalgh, C. (2015). Social access vs. privacy in wearable computing: A case study of autism. *Pervasive Computing* , 26-33.
[36] Krupp, J., Schröder, D., & Simkin, M. (2014). Enhancing security and privacy with Google glass. *CCS '14 Proceedings of the ACM Conference on Computer and Communications Security* (pp. 1445-1447). New York: ACM.
[37] Larson, K. (1998). The role of service level agreements in IT service delivery. *Information Management and Computer Security* , 128-132.
[38] Li, H., Wu, J., Gao, Y., & Shi, Y. (2016). Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective. *International Journal of Medical Informatics* , 8–17.
[39] Li, J., Chen, X., Li, J., Jia, C., Ma, J., & Lou, W. (2015). New access control systems based on outsourced attribute-based encryption. *Journal of Computer Security* , 659-683.
[40] Liberati, A., Altman, D., Tetzlaff, J., Mulrow, C., & Gøtzsche, P. (2009). The PRISMA Statement for Reporting Systematic Reviews and Meta-Analyses of Studies That Evaluate Health Care Interventions: Explanation and Elaboration. *PLoS Medicine* .
[41] Macintosh, A. W. (2008). Towards an evaluation framework for eParticipation. *Transforming government: People, Process & Policy,* , 16-30.
[42] Malhotra, K., Kim, S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research* , 336-35.
[43] Malhotra, N., Kim, S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research* , 336-355.
[44] Mason, R. (1986). Four ethical issues of the information age. *MIS Quarterly: Management Information Systems* , 5-12.
[45] Moher, D., Liberati A, ,. A., Tetzlaff, J., & Altman, D. (2009). Preferred Reporting Items for Systematic

Reviews and Meta-Analyses: The PRISMA Statement. *PLoS Medicine* .
[46] Moore, D., Shannon, C., Brown, D., Voelker, G., & Savage, S. (2006). Inferring internet denial-of-service activity. *ACM Transactions on Computer Systems (TOCS)* , 115-139.
[47] Motti, V., & Caine, K. (2015). Users' privacy concerns about wearables: Impact of form factor, sensors and type of data collected. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* , 231-244.
[48] Mouton, F., Malan, M. M., Leenen, L., & Venter, S. H. (2014). Social engineering attack framework. *Information Security for South Africa (ISSA), 2014* (pp. 1-9). Johannesburg: IEEE.
[49] Moynihan, D. (2003). Normative and Instrumental Perspectives on Public Participation Citizen Summits in Washington, D.C. *American Review of Public Administration* , 164 - 188.
[50] Oliveira, T., & Martins, M. (2010). Information technology adoption models at Firm Level: Review of literature. *4th European Conference on Information Management and Evaluation* (pp. 312-322). Lisbon: ECIME.
[51] Pagani, M. (2004). Determinants of adoptionof third generation mobile multimedia services. *Journal of Interactive Marketing* , 46-59.
[52] Palen, L., & Douris, P. (2003). Unpacking "privacy" for a networked world. *SIGCHI conference on Human factors in computing systems* (pp. 129–136). New York: ACM.
[53] Pavlou, P., Huigang, L., & Yajiong, X. (2007). Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective. *MIS Quarterly* , 105-136.
[54] Qin, L., Yongbcom, K., Xin, T., & Jerffrey, H. (2009). The Effects of Privacy Concern and Social Influence on User Acceptance of Online Social Networks. *Americas Conference on Information Systems* (pp. 885-899). San Francisco: AISel.
[55] Rogers, E. (1995). *Diffusion of innovations.* New York: Free Press.
[56] Rossi, B. (2014, April 1). *85% of the public sector is unprepared for the impact of wearable technology on its IT infrastructure.* Retrieved May 18, 2016, from Information Age: http://www.information-age.com/technology/data-centre-and-it-infrastructure/123457858/85-public-sector-unprepared-impact-wearable-technology-its-it-infrastructure
[57] Russell, J. (2003). Core Affect and the psychological construction of emotion. *Psychological Review* , 145-172.
[58] Schilit, B., & Theimer, M. (1994). Disseminating active map information to mobile hosts. *IEEE Network* , 22-32.
[59] Schryen, G. (2015). Writing Qualitative IS Literature Reviews—Guidelines for Synthesis, Interpretation, and Guidance of Research. *Communications of the Association for Information Systems* .
[60] Shin, D. (2009). Understanding user acceptance of DMB in South Korea using the modified technology acceptance model. *International Journal of Human-Computer Interaction* , 173-198.
[61] Shin, D. (2012). What makes consumers use VoIP over mobile phones? Free riding or consumerization of new service. *Telecomunications Policy* , 311-323.
[62] Silic, M., & Back, A. (2014). Information security: Critical review and future directions for research. *Information Management & Computer Security* , 279 - 308.
[63] Skorodumov, B., Skorodumova, O., & Matronina, L. (2015). Research of human factors in information security. *Modern Applied Science* , 287-294.
[64] Smith, A., Papadaki, M., & Furnell, S. (2013). Improving awareness of social engineering attacks. *8th IFIP WG 11.8 World Conference on Information Security Education* (pp. 249-256). Auckland: Springer.
[65] Srite, M., & Karahanna, E. (2006). The Role of Espoused National Cultural Values in Technology Acceptance. *MIS Quarterly* , 679-704.
[66] Staff, M. C. (2014, December 3). *Adoption Factors for Wearable Technology across Industry Verticals*. Retrieved June 2, 2016, from MARKET RESEARCH INSIGHTS & BUSINESS INTELLIGENCE: http://blog.marketresearch.com/adoption-factors-for-wearable-technology-across-industry-verticals
[67] Statista. (2016, May 18). *Number of smartphone users in the United States from 2010 to 2019 (in millions)** . Retrieved May 18, 2016, from Statista: http://www.statista.com/statistics/201182/forecast-of-smartphone-users-in-the-us/
[68] Suki, N., & Ramayah, T. (2011). Understanding consumer intention with respect to purchase and use of pirated software. *Information Management and Computer Security* , 195-210.
[69] Sundar, S., Tamul, D., & Wu, M. (2014). Capturing 'cool': measures of assessing coolness of technological products. *International Journal Of Human-Computer Studies* , 169-180.
[70] Thomas, J. C. (2003). The New Face of Government: Citizen Initiated Contacts in the Era of E-Government. *Journal of Public Administration Research and Theory* , 83-102.
[71] Thomaz, E., Parnami, A., Bidwell, J., & Abowd, G. (2013). Technological approaches for addressing privacy concerns when recognizing eating behaviors with wearable cameras. *ACM international joint conference on Pervasive and ubiquitous computing* (pp. 739-748). New York: ACM.

[72] Thorp, E. (1998). The Invention of the First Wearable Computer. *ISWC '98 Proceedings of the 2nd IEEE International Symposium on Wearable Computers* (pp. 4-8). Washington, DC: IEEE.
[73] Tornatzky, L., & Fleischer, M. (1990). *The processes of technological innovation.* Lexington: Lexington books.
[74] Trelease, R. (2006). Diffusion of innovations: Anatomical informatics and iPods. *The Anatomical Record* , 160- 168.
[75] Venkatesh, V., Morris, ,. M., Davis, G., & Davis, F. (2003). User acceptance of information technology: toward a unified view. *MIS Quarterly* , 425-478.
[76] Webster, J., & Watson, R. (2002). ANALYZING THE PAST TO PREPARE FOR THE FUTURE: WRITING A LITERATURE REVIEW. *MIS Quarterly* .
[77] William, S. (2011). *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker.* New York: Little, Brown and Company.
[78] Xiaofeng, L., Zhaowei Qu, ,. Q., Qi Li, L., & Pan, H. (2015). Privacy Information Security Classification for Internet of Things Based on Internet Data. *International Journal of Distributed Sensor Networks* .
[79] Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. *Journal of the Association for Information Systems* , 798-824.
[80] Yiwen, G., He, L., & Yan, L. (2015). An empirical study of wearable technology acceptance in healthcare. *Industrial Management & Data Systems* , 1704 - 1723.
[81] Ziamou, P., & Ratneshwar, S. (2002). Promoting consumer adoption of high-technology products: Is more information always better? *Journal of Consumer Psychology* , 341-351.