The Effect of Data Security Perception on Wearable Device Acceptance: A Technology Acceptance Model.

Abigail DuFour
Pace University
Pleasantville, NY
ad62376n@pace.edu

Kelly Lajeunesse
Pace University
Pleasantville, NY
kl13166p@pace.edu

Rushabh Pipada
Pace University
New York, NY
rp88801n@pace.edu

Shijian Xu
Pace University
Pleasantville, NY
sx68157n@pace.edu

***Abstract*— Every device added to the Internet of Things is an additional point of entry for hackers and a security risk to consumers. Wearable devices in particular create a vast amount of personal data which needs to be protected. The Technology Acceptance Model shows how users may come to use and accept new technologies by measuring perceived usefulness and perceived ease of use. This study uses survey results to gauge consumer concern regarding data security for wearable devices, and explores whether these security concerns can be successfully accommodated into the Technology Acceptance Model.**

***Index Terms*— Technology Acceptance Model, Wearable Devices, Data Security, Internet of Things.**

I. Introduction

COMMERCIAL wearable computing devices have become part of mainstream culture. With one in six Americans currently using a smart watch or fitness tracker, wearable technology is becoming increasingly ubiquitous. It is predicted that 19 million fitness devices will be sold worldwide in 2016 and by 2018 that number will reach 110 million sold [11]. Starting with the FitBit for fitness tracking, through the Samsung Gear and Motorola Moto360 which give text, email, weather, and many Android Wear apps, to the Apple Watch with Apple Pay NFC capability on the wrist, there is an almost overwhelming choice of products available on the consumer market.

One of the popular claims of all these devices is that they will promote good habits: better fitness, better nutrition, breaking bad habits, being on time and informed. This is done through a combination of reading a number of different behavioral and physiological sensors on the "smartwatches", and software released by the smartwatch distributors and independent app developers: Google Fit, Apple Health, Microsoft Health. One argument for the advantages of smartwatches over smartphones in this area is that the smartwatch is in constant contact with your skin and sensor information can be read continuously. Also, haptic feedback (vibration) to get your attention is more effective on the wrist than on a phone. Smart devices are an ever increasing consumer product with remarkable potential for users.

Perception plays a large role in the choice of the consumer as to whether they ultimately purchase a wearable device. The Technology Acceptance Model (TAM) delineates these perceptions into two categories: perceived usefulness and perceived ease of use. Our goal is to explore the functionality of TAM to determine in what way perceptions of data security issues could play a role in that model, and additionally what role that concern may have with consumer perceptions. We will accomplish this by performing a survey and tabulating the results to determine what impact, if any, concerns of data security have on consumers of wearable devices.

II. Background

Smartwatches are one of the latest developments in the evolution of information technology wearables and have a seemingly infinite number of apps to increase functionality. One popular application is the delivery of text messages and call notifications to the smartwatch. In a time when the average connected individual is part of 22 phone calls and 23 messages every day, the utility of having notifications readily available on one's wrist is of ever-increasing importance [3]. Smartwatches are also being used to increase quality of life for dementia patients [3]. Smartwatches and wearable devices are used in myriad applications in different markets.

The market for the technology of wearables is growing. IDC (2015a) predicts the worldwide market for wearables will reach more than 111 million units in 2016, an increase of 44% compared to 2015. More than eighty percent of these devices will be wrist-worn, i.e., smartwatches or smart fitness watches. A trend analysis in the search engine Google reflects a tremendous increase in searches for "smartwatch" and related terms, supporting the results of the market research. The increase in the amount of apps offered for smartwatches, such as 10,000 for the Apple Watch and more than 4,000 for 'Android Wear' also supports this research (Curry,2015).

Although reports have forecast an increased demand for smartwatches in the future, the market has begun to cool off as consumers become impatient with the technology's lack of distinct capabilities, such as LTE connectivity and device specific apps. Consumers desire that smart watches needs to have three specific qualities: good functionality, stylish

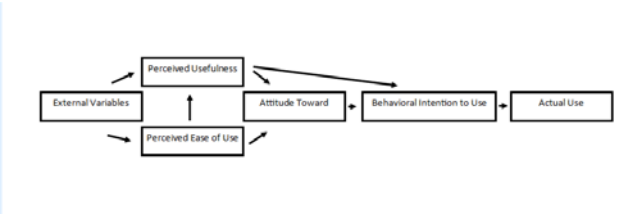
appearance, and a relatable product line [5]. Is this what actually drives the adoption of smart devices? Previous technology acceptance research developed various frameworks to study consumers' acceptance of new technology, such as the technology acceptance model, (TAM) (King&He, 2006). However, seemingly no research has been done to study smartwatches through the lens of TAM and the effect of data security perceptions on wearable device acceptance.

2. Technology Acceptance Model

Research on technology acceptance models started in the 1980s. One of the most prominent models in this area was the technology acceptance model (TAM), which was developed by Davis (Davis, 1989). TAM was derived from the theory of reasoned action (TRA; Ajzen & Fishnein, 1980). The model explains the acceptance of technology through measuring individuals' intentions to use a technology and determining factors. Holden and Karsh (2010) point out that in order to promote technology acceptance and even increase technology use, knowing which of the factors negatively influence technology acceptance would help organizations to better control those factors.

TAM defines behavioral intention or acceptance by two important factors: perceived ease of use (PEOU) and perceived usefulness (PU). Perceived usefulness is defined as "the degree to which a person believes that using a particular system would enhance his or her performance" Perceived Ease of Use is defined as "the degree to which a person believes that using a particular system would be free of effort," (Davis, 1989).

Figure 1: The Technology Acceptance Model



Both PU and PEOU influence the attitude towards use of technology (ATT) which in turn influences the behavioral intention to use (BI). The only difference is that PU has a direct effect on BI. The model highlights a causal relationship of PEOU on PU (perceived ease of use is shown to affect perceived usefulness). In the model, BI or acceptance will lead to actual use (AU). However, compatibility has a significant effect in consumer technology acceptance decision (Rogers, 1995). Compatibility to the degree by which an innovation is seen as consistent with existing values, past experiences, and needs of potential adopters impacts technology acceptance [16].

3. Applications and Security

There are two kinds of applications which give particular rise to consumer security concerns. The first kind is designed to gather information about a user. Some examples are social media applications such as Facebook, which skillfully endeavor to draw as much information about their users as possible. This can be advantageous for both users and companies by users getting more involved with their network and companies get more information to sell to advertisers.

The second type of application which poses a considerable data security risk are, counterintuitively, the very apps which advertise themselves as specifically dedicated to preserving user privacy. Snap Chat is a clear example of this, having long claimed that it is dedicated to anonymity and user-data protection, and yet was subject to multiple information leaks. Additionally, applications like Snap Chat lure users into a false sense of security, which in turn prompts users to allow more of their information to be used without realizing the complete details of a company's privacy policy.

Wearable devices exaggerate these problems, because their applications run in the background of a device, constantly drawing in new information about a user whether or not they are actively using it at that time. Another problem is that these applications are being used in real time. Consumers no longer rely on a stationary desktop computer, or occasionally checking in on a previous mobile device, devices are now worn and used on the go. This creates a considerable volume of data and metrics on each user, and all of this data must be kept secure. In addition, few people will read the privacy policies that are associated with their wearable. Failure to do so results in the user being unaware of how their wearable device stores, manages and protects personal information [12].

The data that is collected through wearable devices such as a Fitbit or smartwatch means that there are tangible risks involved. If this data is carelessly stored, and then stolen through a data breach and sold to an unscrupulous organization that is willing to use that data to access health risks, a consumer could possibly face steep increase in health insurance. This risk is so real that some companies are opting to protect themselves by buying data breach insurance. This also opens the company to a potential lawsuit from customers who believe their data to be held at a high level of security [17].

With the growing fear of data security breaches as each new item is added to the vast landscape of the Internet of Things, it is increasingly important to develop a clear understanding of whether a TAM model can successfully accommodate consumer concerns about data security within the categories of PU and PEOU, or whether another model must be utilized.

III. Methodology

The main goal of the survey was to gather baseline data to identify the genders and ages of the respondents, assess their initial levels of interest in wearable fitness devices and level of concern about data security, and ask questions relevant to how

data security risks might alter their desire to use a wearable fitness tracker. Two questions are repeated at the beginning and end of the survey in order to assess whether the process of taking the survey was enough to alter interest in wearable fitness trackers and/or level of concern about data security.

A. Question Formatting:

The survey was constructed utilizing the BRUSO method of survey construction. BRUSO stands for Brief, Relevant, Unambiguous, Specific, and Objective. Brief surveys are succinctly worded and short in length to maximize subject completion rates. BRUSO was accomplished by constructing terse questions and narrowing down the questions asked to a list of the twelve most important to our study [13].

B. Data Collection:

We utilized both our social networks and the collection features of the internet survey website Surveymonkey to acquire a sufficient population sample encompassing all target age ranges (18-70+) and a solid sample of each gender (55% male and 44% female). The respondents were given closed answers to each question and we had an abandon rate of 13% which is reasonable.

C. Survey *Questions:*

1. What is your gender? (Female, Male)
2. What is your age? (18 to 24, 25 to 34, 35 to 44, 45 to 54, 55 to 64, 65 to 74, 75 or older)
3. Do you own a wearable fitness tracker (Fitbit, Samsung Gear, Garmin Vivofit, Apple Watch, Bodymedia Fit, ect.)? (Yes No)
4. How interested are you in purchasing a wearable fitness tracker? (Uninterested, Somewhat Interested, Interested, Very Interested, Extremely Interested)
5. How concerned are you with the security of your data? (Unconcerned, Somewhat Concerned, Concerned, Very Concerned, Extremely Concerned)
6. If you heard that a wearable fitness tracking company had one data security breach in the past twelve months where no personally identifying information was taken (i.e. name, address, location data), how likely would you be to purchase that brand today? (Much less Likely, Somewhat Less Likely, Equally Likely, Would Purchase a Different Brand, Would Not Purchase Any Brand)
7. If you heard that a wearable fitness tracking company had one data security breach in the past twelve months where personally identifying information was taken (i.e. name, address, location data), how likely would you be to purchase that brand today? (Much Less Likely, Somewhat Less Likely, Equally Likely, Would Purchase a Different Brand, Would Not Purchase Any Brand)
8. If you heard that a wearable fitness tracking company had multiple data security breaches in the past twelve months where personally identifying information was taken (i.e. name, address, location data), how likely would you be to purchase that brand today? (Much Less Likely, Somewhat Less Likely, Equally Likely, Would Purchase a Different Brand, Would Not Purchase Any Brand)
9. To what extent, if any, do you feel data security impacts the ease of using fitness trackers? (Does Not Impact Ease of Use (0) - Significantly Impacts Ease of Use (100))
10. To what extent, if any, do you feel data security impacts the usefulness of fitness trackers? (Does Not Impact Usefulness (0) - Significantly Impacts Usefulness (100))
11. How concerned are you with the security of your data? (Unconcerned, Somewhat Concerned, Concerned, Very Concerned, Extremely Concerned)
12. How interested are you in purchasing a fitness tracker? (Uninterested, Somewhat Interested, Interested, Very Interested, Extremely Interested)

IV. Results

The survey accumulated 104 complete responses. Gender of responders was skewed slightly in favor of females. The ages of those surveyed was well balanced across all age ranges.

Figure 2: Question 1 Responses

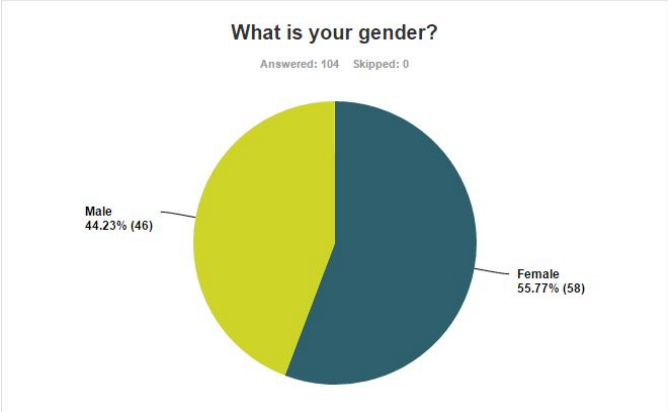
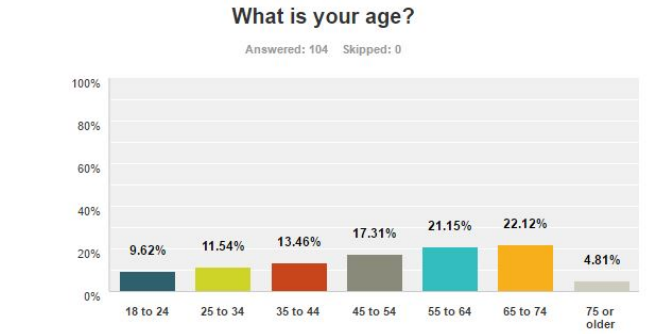


Figure 3: Question 2 Reponses



Thirty-one responders owned a wearable fitness tracker, while 73 did not own one. Half of those surveyed were not interested in purchasing a wearable fitness tracker, while the other half varied in their degree of interest.

Figure 4: Question 3 Responses

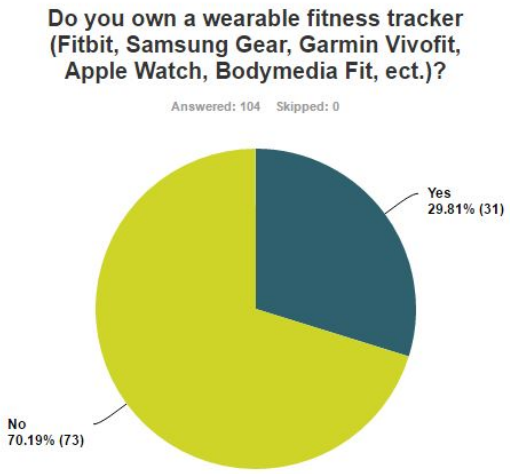
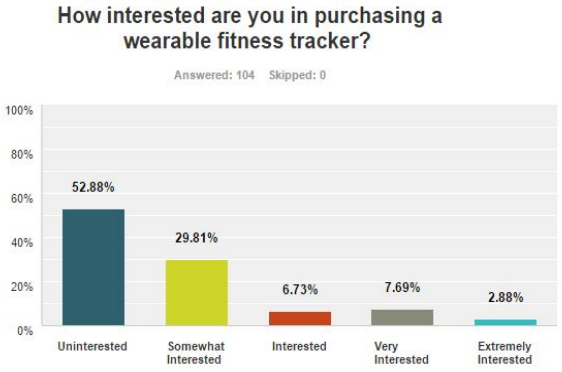


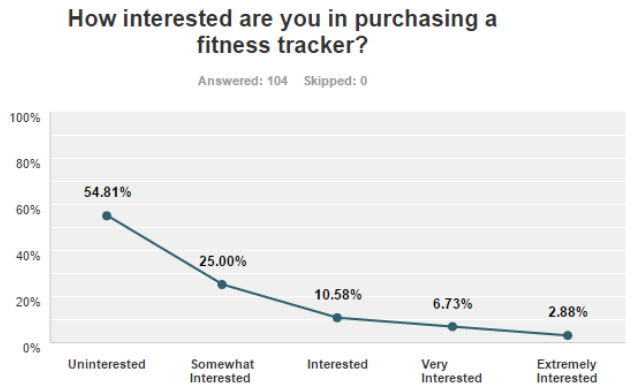
Figure 5: Question 4 Responses



The question in Figure 5, "How interested are you in purchasing a wearable fitness tracker?" was one of two questions asked both at the beginning and the end of the survey. The purpose of this was to determine if the act of taking the survey and thinking about data security would be enough to change the degree to which a respondent might be interested in purchasing a wearable fitness device.

Figure 6 Question 4 Responses

Figure 7 Question 12 Responses



Those surveyed were asked the question, "How concerned are you about the security of your data?" both at the beginning and end of the survey. The purpose of this was to determine if the process of answering questions and thinking in general about data security issues would decrease the level of interest in those responding. The results ran counter to this hypothesis, with nearly an identical level of interest at each level, and a slight uptick in moderate levels of interest. In general, as shown in figures 6 and 7, the results were nearly identical suggesting that data security fears do not have a strong impact on product interest.

The other question that was asked twice, was question five and eleven, "How concerned are you with the security of your data?" Eight percent of responders moved their votes from the unconcerned/somewhat concerned range into the concerned/veryconcerned/extremely concerned range. This was a significant enough number where it does appear that simply contemplating data security risks does appear to increase the level of concern about data security in some responders.

Figure 8: Question 5 and 11 Responses Line Graph

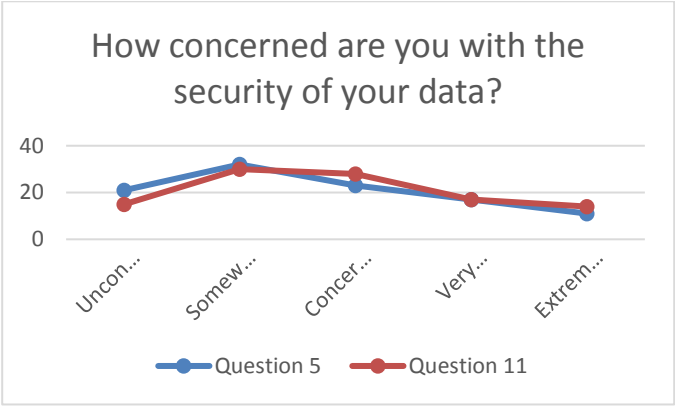
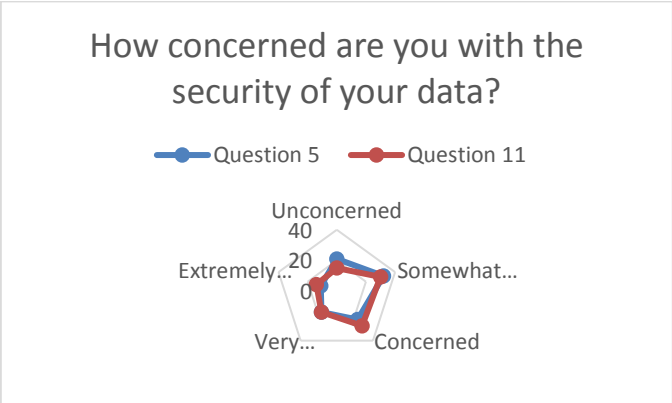
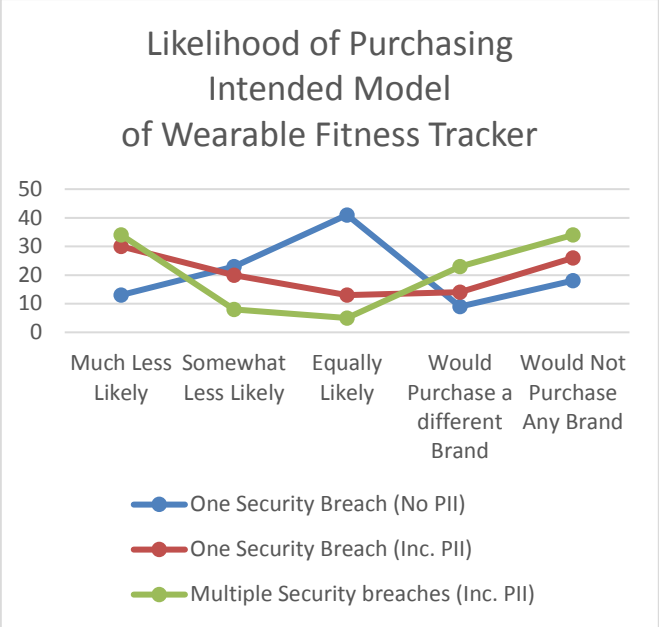


Figure 9: Question 5 and 11 Responses Radar Diagram



The next set of questions, questions 6-8, explore customer purchasing response to data security breaches for wearable fitness trackers. In Figure 10, a line is plotted for each of the three breach scenarios which were presented to responders. In the first scenario, the company they are planning to purchase from has had one data breach in the past twelve months in which no personally identifying information (PII). In the second scenario, one data breach occurred in the past twelve months where PII was released. In the third scenario the company has had multiple data breaches in the past twelve months where PII was taken.

Figure 10: Question 6-8 Responses



Responses clearly trended towards "much less likely" and "would not purchase any brand" in correlation with the increasing levels of data breaches occurring. Initially, 39% of responders were equally likely to purchase their favored product regardless of the security breach, however in question seven when that data breach included the release of PII, this number dropped to 12.6%. Finally when the third scenario was presented in question eight, where multiple data breaches had occurred in the past twelve months which released PII, the numbed dropped still lower to just 4.81% of responders planning to still buy their chosen product. Correspondingly, the percentages of responders who would not purchase any brand increased from 17%, 25%, to 33% for those same three scenarios. These data trends suggest that data security does have a measurable impact upon technology acceptance for consumers.

Figure 11: Question 6 & 8 Responses

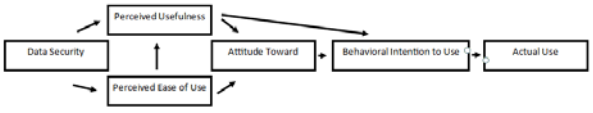
	One Security Breach (No PII)	Multiple Security breaches (Inc. PII)
Much Less Likely	13	34
Somewhat Less Likely	23	8
Equally Likely	41	5
Would Purchase a different Brand	9	23
Would Not Purchase Any Brand	18	34

Questions Nine and Ten relate the most directly to the TAM model. Question Nine asks about PU and Question Ten asks about PEOU, both in regards to data security. In Question Nine, the survey asked, "To what extent, if any, do you feel data security impacts the ease of using fitness trackers?" and Question Ten asked, "To what extent, if any, do you feel data security impacts the usefulness of fitness trackers?" Responses were given on a 100 point scale where 0 represented no impact and 100 represented significant impact. The results for Question Nine were a mean of 32 and a median of 18. The results for Question Ten were a mean of 36 and a median of 24.5.

IV. Conclusions

We believe that the results regarding PU and PEOU in questions nine and ten, as well as the data trends across questions six – eight, show that data security has a moderate level of impact on technology acceptance for consumers and does affect their behavioral intention to use. Data security concerns affect Perceived Ease of Use, Perceived Usefulness, and Attitude Toward wearable devices. As such, data security becomes a significant factor to take into account when modelling user acceptance of wearable fitness trackers.

Figure 12: Data Security & TAM for Wearable Devices



Although scope did not allow for a further exploration of how data security regarding wearable devices could be incorporated into models like TAM2 and UTAUT, we see this as a promising avenue for future studies.

REFERENCES

[1] *A. Karahanoğlu and Ç. Erbuğ, "Perceived qualities of smart wearables,"Proceedings of the 2011 Conference on Designing Pleasurable Products and Interfaces - DPPI '11, 2011.*

[2] *A. Lunney, N. R. Cunningham, and M. S. Eastin, "Wearable fitness technology: A structural investigation into acceptance and perceived fitness outcomes," Computers in Human Behavior, vol. 65, pp. 114–120, 2016.*

[3] *B. Spencer for the Daily Mail, "Mobile users can't leave their phone alone for six minutes and check it up to 150 times a day," Daily Mail Online, Nov-2013. [Online]. Available: http://www.dailymail.co.uk/news/article-2276752/Mobile-users-leave-phone-minutes-check-150-times-day.html. [Accessed: 11-Dec-2016].*

[4] *C. Boletsis, S. Mccallum, and B. F. Landmark, "The Use of Smartwatches for Health Monitoring in Home-Based Dementia Care," Lecture Notes in Computer Science Human Aspects of IT for the Aged Population. Design for Everyday Life, pp. 15–26, Jul. 2015.*

[5] *D. Pradhan and N. Sujatmiko, "Can smartwatch help users save time by making processes efficient and easier," thesis, 2014.*

[6] *E. M. Rogers, Diffusion of innovation. London: The Free Press, 1982.*

[7] *H. Z. Cheng, "HP Study Reveals Smartwatches Vulnerable to Attack," The Tech Revolutionist, 01-Aug-2015. [Online]. Available: http://www.thetechrevolutionist.com/2015/08/hp-study-reveals-smartwatches.html. [Accessed: 11-Dec-2016].*

[8] *H., Chanmi, "Consumers' acceptance of wearable technology: Examining solar-powered clothing" (2014). Graduate Theses and Dissertations. Paper 13950.*

[9] *J. Schepers and M. Wetzels, "A meta-analysis of the technology acceptance model: Investigating subjective norm and moderation effects," Information & Management, vol. 44, no. 1, pp. 90–103, 2007.*

[10] *K. J. Kim and D.-H. Shin, "An acceptance model for smart watches," Internet Research, vol. 25, no. 4, pp. 527–541, Mar. 2015.*

[11] *L. Piwek, D. A. Ellis, S. Andrews, and A. Joinson, "The Rise of Consumer Health Wearables: Promises and Barriers," PLOS Medicine, vol. 13, no. 2, Feb. 2016.*

[12] *M. Wright, "The Dark Side Of Wearable Tech: Should You Be Worried? - Brandwatch," Brandwatch, 17-Nov-2014. [Online]. Available: https://www.brandwatch.com/blog/dark-side-wearable-tech/. [Accessed: 11-Dec-2016].*

[13] *R. A. Peterson, Constructing effective questionnaires. Thousand Oaks: Sage Publications, 2000.*

[14] *R. Sol and K. Baras, "Assessment of activity trackers," Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing Adjunct - UbiComp '16, 2016.*

[15] *S. H.-W. Chuah, P. A. Rauschnabel, N. Krey, B. Nguyen, T. Ramayah, and S. Lade, "Wearable technologies: The role of usefulness and visibility in smartwatch adoption," Computers in Human Behavior, vol. 65, pp. 276–284, 2016.*

[16] *S. Nasir and Y. Yurder, "Consumers' and Physicians' Perceptions about High Tech Wearable Health Products," Procedia - Social and Behavioral Sciences, vol. 195, pp. 1261–1267, Jul. 2015.*

[17] *T. Maddox, "The dark side of wearables: How they're secretly jeopardizing your security and privacy - TechRepublic," TechRepublic, 17-Apr-2016. [Online]. Available: http://www.techrepublic.com/article/the-dark-side-of-wearables-how-theyre-secretly-jeopardizing-your-security-and-privacy/. [Accessed: 11-Dec-2016].*

[18] *V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User Acceptance of Information Technology: Toward a Unified View," MIS Quarterly, vol. 27, no. 7, pp. 425–478, Sep. 2003.*