Journal of King Saud University – Computer and Information Sciences 31 (2019) 497–505

Contents lists available at ScienceDirect

Journal of King Saud University – Computer and Information Sciences

journal homepage: www.sciencedirect.com

A model for predicting user intention to use wearable IoT devices at the workplace

Huseyin Yildirim [a,b], Amr M.T. Ali-Eldin [a,c,*]

[a] Leiden Institute of Advanced Computer Science, Leiden University, P.O. Box 9512, 2300 RA Leiden, The Netherlands
[b] CGI Nederland, George Hintzenweg 89, Rotterdam, The Netherlands
[c] Computer and Control Systems Engineering Department, Faculty of Engineering, Mansoura University, Mansoura, Egypt

ARTICLE INFO

Article history:
Received 28 November 2017
Revised 26 February 2018
Accepted 1 March 2018
Available online 2 March 2018

Keywords:
Behaviour intention
Privacy
Trust
Wearable devices
Internet of Things (IoT)
Adaptive Neuro-Fuzzy Inference systems (ANFIS)
Partial Least Square Modelling (PLS)

ABSTRACT

The internet of things refers to devices that are connected to the Internet and communicate with each other providing many benefits to users, but they could also violate their privacy. The main objective of this study is to analyse the factors that influence employees' intention to use wearable devices at the workplace. In this study, a review of the literature regarding acceptance of technologies and influencing factors such as risk and trust is used to develop a conceptual model. The proposed conceptual model was tested using a survey conducted among employees of an IT consulting firm, with a total of 76 participants. Partial least square path and Adaptive Neuro-Fuzzy Inference modelling were used to validate and predict these factors influence on users' intention to use these devices. The findings indicate that the perceived usefulness of a wearable IoT device provides the strongest motivation for individuals to use it at the workplace. Further results show that applying the ANFIS approach helps improve the predictability of user intention to use IoT devices.

1. Introduction

Internet of Things (IoT) brings many different kinds of devices into the market which collect, process and distribute data such as security cameras with face recognition technology, sport watches with GPS and smart homes. According to Gartner (2016a), the use of Internet of Things (IoT) devices has dramatically increased in the last few years and the number of sold wearable devices is growing fast since 2015. Further, Gartner predicts that by 2020 about 21 billion devices will be connected, compared to 6.4 billion in 2016 (Gartner, 2016b).

Wearable devices can bring many benefits to the users, but they could also harm users' privacy without their notice. These wearable devices are used for entertainment and to enhance the quality of life. Morris (2015) defines wearable devices as electronics or computers that can be worn on the body when inserted into items of clothing and accessories. Examples of wearable devices are smart clothes, smart motorbikes helmets, smart bands and eye glasses (Morris, 2015). Wearable devices were mainly used in the military field, but are also becoming more common in various fields such as gaming, and especially in healthcare (Tehrani and Michael, 2014). In the field of healthcare, wearable devices include features such as health monitoring, exercise patterns, sleep patterns and heart pattern recording (Morris, 2015). Regarding monitoring of sleeping patterns and physical activity, smart bands are the most used wearable devices (miCoach, 2015).

Wearable devices collect significant amount of information and raise a number of privacy concerns. It is not clear where the information goes, what is being done with it and who collects the information (Flaherty, 2014). Nevertheless, many employers adopt them for work purposes which is raising many societal concerns (Hamblen, 2015). Despite that the use of wearable devices can cause threats to users privacy, these devices bring benefits to employers and individuals. Thus, there is always a trade-off between risks associated with the use of such technology and perceived benefits.

In this study, we address the above mentioned issues by proposing a conceptual model that defines factors influencing users' intention to use wearable devices at the workplace. This

* Corresponding author.
E-mail address: a.m.t.ali-eldin@liacs.leidenuniv.nl (A.M.T. Ali-Eldin).

Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

https://doi.org/10.1016/j.jksuci.2018.03.001
1319-1578/

model provides an understanding of the different factors that influence users' intention to use wearable devices at the workplace namely individuals' privacy concerns regarding information and additional factors such as risk, trust and perceived usefulness. The paper is outlined as follows: next section presents literature review. Next, the proposed model is introduced in Section 3 followed by explanation of the data collection and analysis in Sections 4 and 5 respectively. Section 6 provides an overview of the obtained results followed by a discussion in Section 7. Section 8 concludes the paper providing highlights on possible future work.

2. Literature review

This study focuses on individuals' behavioural intention to use wearable devices at work. The effectiveness of wearable devices in this context depends on the intended users' acceptance and actual use of the technology. Acceptance of technology has been heavily researched in the literature offering many definitions (Dillon and Morris, 1996; Elaklouk et al., 2015). Literature studies in information systems have led to the development of several theoretical models in psychology, sociology and information systems (Venkatesh et al., 2003). Currently, these theoretical models focus mainly on the acceptance of technology in general. This research is focused on the acceptance of wearable devices at the individual level in organizations and understanding which theoretical characteristics may be important in this process. The theoretical models that explore the acceptance of technology in this area are the theory of planned behaviour (Ajzen, 1985), the theory of reasoned action (Fishbein and Ajzen, 1975) and the technology acceptance model (Davis, 1989).

The Theory of Reasoned Action (TRA) attempts to explain the relationship between a person's attitude and behaviour in order to make predictions about his or her actions. According to the TRA (Fishbein and Ajzen, 1975), the intention of an individual is predicted by two variables, namely the attitude and the subjective norm. Technology acceptance model (TAM) (Davis, 1989), adapted from the Theory of Reasoned Action (TRA), is one of the most prominent in the area of technology acceptance models. The model explains the acceptance of technology by measuring the intention of individuals to use a technology, and determining factors that could influence their decision (Davis, 1989; Fishbein and Ajzen, 1975). The Technology Acceptance Model (TAM) includes two important factors to determine an individual's intention or acceptance toward using a technology, namely perceived usefulness (PU) and perceived ease of use (PEOU). Perceived usefulness is defined by Davis (1989) as "the degree to which a person believes that using a particular system would enhance his or her job performance", while perceived ease of use refers to "the degree to which a person believes that using a particular system would be free of effort". According to the model, perceived usefulness affects an individual's attitude toward using a technology and also his or her intention toward using the technology. Perceived ease of use affects the perceived usefulness and has a direct influence on attitude. TAM is helpful in predicting people's acceptance of technology at work, and it has become one of the most used technology models in literature (Venkatesh et al., 2003).

The updated model, known as TAM2 (Venkatesh and Davis, 2000), added five factors, to the original model, that influence PU. These factors are subjective norm, image, job relevance, output quality and result demonstrability. The unified theory of acceptance and use of technology (Venkatesh et al., 2003) is an extension of the original technology acceptance model. Venkatesh et al. (2003) reviewed eight existing acceptance models, and concluded that four main constructs influence a user's intention of using an information system: performance expectancy, effort expectancy, social influence and facilitating conditions. Performance expectancy is the degree to which an individual believes that a system will help him or her improve his or her job performance. Effort expectancy is similar to the perceived ease of use of the original technology acceptance model; it is the degree to which a person believes that using a particular system would be free of effort (Davis, 1989). Social influence describes the individual's belief that other people will also use the system. Lastly, facilitating conditions are the degree to which an individual believes that organizational and technical infrastructure supports the use of the system. Finally, in the model, the intention toward using a system is determined by gender, age, experience and voluntariness.

3. The proposed conceptual model

Fig. 1 shows the proposed conceptual model with factors influencing behavioural intention to use IoT wearable devices at work. In the following, these factors are presented.

3.1. Concerns for information privacy (CFIP)

The growing influence of technology on daily life has caused many concerns about privacy, particularly with regards to how information is collected and transferred through the internet. Privacy is a multidisciplinary problem which was heavily discussed by many scholars in the literature (Campbell, 1997; Clarke, 1999; Fried, 1970; Mason, 1986; Parent, 1983; Warren and Brandeis, 1890; Westin, 1968). Clarke (1999) categorizes privacy into four subtypes; physical, organisational, personal and data privacy. More information on this can be found in (Clarke, 1999; Fried, 1970; Parent, 1983). For most people privacy feels as a form of power, to have full control over own personal information and life (Ali Eldin and Wagenaar, 2007; Parker, 1973).

Privacy concerns used in this study are based on those developed by Smith et al. (1996) and are presented by concerns for collection of personal information (Col), concerns for errors in collected personal information (Err), concerns for unauthorized secondary use (SE) and concerns for improper (unauthorized) access to personal data (IA). According to Liu et al. (2005), users'

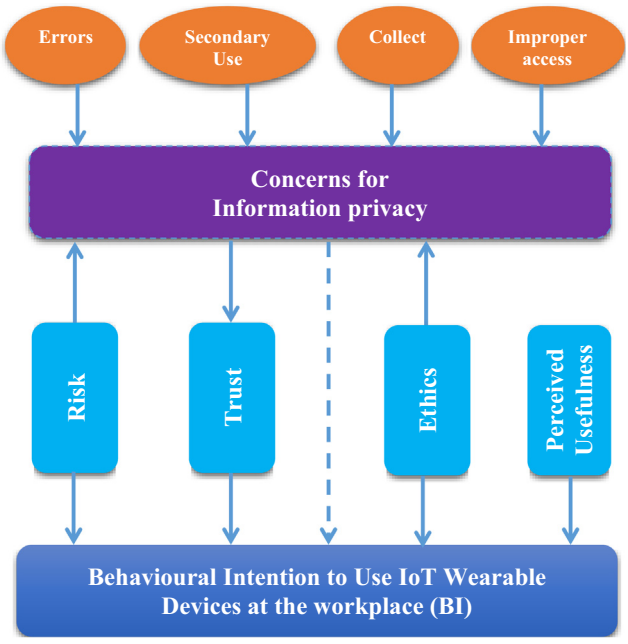

Fig. 1. The proposed conceptual model (arrows represent direction of the effect).

privacy concerns also affect their trust in services being offered, determining their behavioural intention toward using technology. Users with high privacy concerns might doubt the trustworthiness of wearable devices. For example, they are likely to worry about their data being shared with other parties silently. Users with high privacy concerns will have doubts regarding the use of the new technology. Therefore, we expect that CFIP can have a negative impact on their trust in wearable devices and hence on their intension to use the technology.

3.2. Risk

Given that this study focuses on the behavioural intention to use a product, and that people continuously perceive risk when evaluating products for purchase or adoption (Bauer, 1967), risk is a vital concept that must be addressed. Risk is commonly a feeling of uncertainty regarding possible negative consequences when using a product or a service (Schaninger, 1976; Taylor, 1974). Risk is a concept that involves uncertainty and consequences, and has been defined as "a combination of uncertainty plus seriousness of outcome involved" (Bauer, 1967). Peter and Ryan (1976) define risk as the expectation of losses associated with a purchase and they further note that it acts as an inhibitor to purchase behaviour. More studies have defined risk as the expectation and importance of losses (Mowen, 1992). There are five different types of losses: financial, performance, physical, psychological and social. The two major categories of risk identified in (Cunningham, 1964) are performance and psychological. According to Cunningham (1964), risk has six dimensions; performance, financial, opportunity or time, safety, social and psychological loss (however, the threat to privacy replaces safety in the modern context). Since this research focus is on the ICT aspects, the research focus is on privacy risks associated with security vulnerabilities and the leakage of data.

3.3.Trust

According to TRA (Fishbein and Ajzen, 1975), users' beliefs affect their intentions. Thus, belief in trust will affect their behavioural intentions. This study therefore focuses on trust as a vital relationship concept. Trust has been defined heavily in the literature (Gefen et al., 2003; Mayer et al., 1995) where the relationship between trust and information privacy concerns has been defined in different ways (Bansal et al., 2008), but it is still slightly unclear how the role of trust is related to concerns regarding privacy of information. According to previous studies (Ali Eldin and Wagenaar, 2004; Ali Eldin et al., 2004; Dinev and Hart, 2006), trust can be seen as an important factor that influences behavioural intention to use a technology and has a strong effect when compared to information privacy concerns.

3.4. Ethics

People's behavioural intentions and privacy concerns regarding wearable devices can differ for each person. A study of moral or ethical behaviour is therefore required to develop a better understanding of a person's behavioural intention. Moral or ethical behaviour can refer to a wide range of behaviours; this behaviour depends on the perception of individuals, which can differ from person to another (Cole and Smith, 1996; Abdolmohammadi and Baker, 2006). Generally, morality involves judgments of right or wrong and encompasses consistent beliefs about human virtues such as trustworthiness, honesty, respect for authority, sincerity, and a regard for rules and laws (Lifton, 1985). People's moral judgment can vary from culture to culture or organization to another (Aquino, 1998). In this study, morality will be defined as people's norms and values and using wearable devices would be seen as taking risks that personal information will be collected. Individuals who have concerns about this would logically have high privacy concerns and therefore high morality. As a consequence, this will have negative impact on their behavioural intention to use the IoT wearable devices.

3.5. Perceived usefulness

The technology acceptance model (Davis, 1989; Davis et al., 1989) suggests that customer adaptation behaviour is determined by the intention to use a particular system, which, in turn, is determined by the perceived usefulness and ease of use of the system. According to the TAM, perceived usefulness is the degree to which a person believes that using a particular system would enhance his or her job performance. The greater the perceived usefulness of wearable devices, the more likely it is that they will be adopted. Yu-Hui and Stuart (2007) and Yi et al. (2006) found that perceived ease of use and perceived usefulness strongly affect behavioural intentions. This study will, however, only focus on the perceived usefulness of wearable devices, as the survey participants cannot physically test the wearable devices for perceived ease of use but can make an assumption about their usefulness on the basis of a description.

4. Data collection

A survey was distributed amongst the employees of an IT consulting company who are the potential users of wearable devices in this organization. A total of 214 individuals were invited, of which 76 completed the survey. The survey was delivered by e-mail, which included a link to the company's online tool. In the e-mail, the respondents were informed that their responses would be anonymous. All statements were answered, and there were no missing values, as the survey could only be submitted if it was filled in completely.

The online tool used to conduct the survey was the SharePoint environment. This online tool can upload results to the statistical software for analysis. The survey was developed to seek answers to the statements regarding the factors that influence individuals' behavioural intentions of using a wearable device at work. The survey first provides background information on the subject, which is followed by a short scenario wherein the participant is asked to imagine using a wearable device called the Google Glass and the functions of this device are explained. To ensure that the statements for this survey were as valid as possible, they were developed based on the work of scholars who conducted research in relevant theoretical domains. Where possible, statements were adapted from these researches and measured using a 7-point scale, where 1 stands for "strongly disagree" and 7 stands for "strongly agree". The statements of the survey were presented in varying orders. They were adapted from (Davis, 1989; Smith et al., 1996; Jarvenpaa and Tractinsky, 1999; Stewart and Segars, 2002). Table 1 lists all of the research variables used in this survey.

In the interest of validity, items measuring privacy concerns were assessed by the statements developed by (Smith et al., 1996) and adapted to the context of this study. Examples of the statements that were used include "it usually bothers me when companies ask me for personal information" and "when people give personal information to a company for some reason, the company should never use the information for any reason". These concerns are measured and analysed as to whether they have an effect on behavioural intention and trust.

According to Stewart and Segars (2002), information privacy concerns could influence the behavioural intentions of an

Table 1
List of research variables used in survey.

Variable	Reference	Statements/ Questions
Privacy concerns	Smith et al. (1996)	13
Trust	Jarvenpaa and Tractinsky (1999)	6
Risk	Jarvenpaa and Tractinsky (1999)	4
Ethics	Dinev and Hart (2006)	3
Perceived usefulness	Davis (1989)	10
Behavioural intention	Stewart and Segars (2002)	5
Demographics	–	4

individual. Therefore, to measure behavioural intentions, measurement items were adapted to meet the requirements of this study. Examples of the measured statements are "I would be willing to use the Google Glass in the near future" and "once I have a Google Glass, it is very likely that I will make use of it". The measurement items for trust and risk are adapted from the study of (Jarvenpaa and Tractinsky, 1999) to this context. Examples of the statements measured are "I trust that the company would keep my best interests in mind when dealing with my personal information" and "in general, it would be risky to use the device".

The perceived usefulness of the TAM is also measured. The statements are adapted from (Davis, 1989). Examples of the statements that are measured are "I believe the device will be useful in my job" and "the device will make it easier to do my job". The socio-demographics factors for each respondent, such as age, gender, and nationality, were also collected. Previous studies have shown that the age of an individual can negatively influence concerns regarding the privacy of information (Cho et al., 2009; Malhotra et al., 2004; Zukowski and Brown, 2007). The gender of an individual has been shown to influence concerns regarding privacy of information. According to Zukowski and Brown (2007), females are more concerned than males about their personal information and studies have also shown that females demonstrate higher disposition to trust (Graeff and Harmon, 2002). An individual's education is a factor that significantly influences concerns regarding privacy negatively (Zukowski and Brown, 2007). This study does not focus on data gathered from different countries; however, culture is an important factor affecting information privacy concerns, which may result in differences in behaviour and attitude towards privacy between citizens of different nations (Cho et al., 2009; Dinev et al., 2013).

5. Data analysis

Two methods were used to analyse the collected data and to model the relationship between the variables; these are the structural equation model (SEM) technique and Adaptive Neuro Fuzzy Inference System (ANFIS). The partial least squares (PLS) path modelling (Chin, 1998) was used which is a structural equation modelling technique commonly used for testing theoretical assumptions. The SPSS tool was used to analyse the descriptive statistics, and SmartPLS (Ringle et al., 2015) was used to examine the relationships between the variables using the PLS path modelling approach. The steps followed are based on the PLS assessment by (Henseler et al., 2009).

ANFIS (Jang, 1993) is used to create a predictive model that better represents the relationships between the different factors impacting behaviour intention. The ANFIS calculates the output value based on five stages as follows.

Stage one: the fuzzy system maps the input variables to the corresponding fuzzy values. Assuming a number of input variables m and a number of membership functions n, then applying the kth rule as follows ($k = 1,n$):

$$if\ X_1 = X_{1k}\ and\ X_2 = X_{2k} \ldots\ldots and \ldots X_m = X_{nk}$$

$$Then\ f_k = \sum_{j=1}^{m} q_{jk} * X_j + r_j \tag{1}$$

Stage two: target weights are computed from rules firing rates w_k for each rule by the PROD operator:

$$w_k = \prod_{j=1}^{m} w_j \tag{2}$$

Stage three: normalized weights $\overline{w_k}$ are computed:

$$\overline{w_k} = \frac{w_k}{\sum_{k=1}^{m} w_k} \tag{3}$$

Stage four: the target $\overline{f_k}$ is computed as:

$$\overline{f}_k = \overline{w_k} * f_k \tag{4}$$

Stage five: also known as the defuzzification phase is where the final output is computed:

$$f = \sum_{k=1}^{m} \overline{f_k} \tag{5}$$

Further, using a learning mechanism, the parameters q_{kj}, r_j are adapted. The hybrid algorithm (Jang, 1993) is a common learning mechanism and uses two ways; the forward pass and the backward pass. In the forward hybrid algorithm, least square method is used to compute the parameters in stage 4. The backward pass propagates the errors backward and modifies the parameters using gradient descent.

Matlab was used to generate membership functions type and parameters that fit the dataset. To model the input variables, the Gaussian membership function was used such that:

$$f(X, \sigma, c) = e^{\frac{-(X-c)^2}{2\sigma^2}} \tag{6}$$

where, c is the mean, X is the input, and o is the standard deviation. Each input variable is mapped to a fuzzy input $\bar{X}$ such that:

$$\bar{X} = \sum_{k=1}^{n} \mu_k * e^{\frac{-(X-c_k)^2}{2\sigma_k^2}} \tag{7}$$

where μ is membership value.

6. Results

This section presents the results of this study. The first subsection presents the descriptive statistics and discusses several statistics regarding the mean responses of the questionnaires. The second subsection evaluates the reliability and validity of the questions. The third subsection evaluates the relationships within the proposed model. Finally, ANFIS results are presented.

6.1. Descriptive analysis

In total, about 88% males and 12% females completed the survey. In terms of age, 37% of the respondents were in the age range of 45 to 54, and 25% were in the age range of 25–34. Finally, most of the respondents were educated to the bachelor degree level or higher.

6.2. Reliability and validity

In this subsection, the proposed model constructs are tested for reliability and validity. In research using the Partial Least Square (PLS) method, it is more relevant to look at Composite Reliability

(CR) scores because Cronbach's Alpha (Cronbach, 1951) tends to underrate the reliability of the factors (Henseler et al., 2009). However, this study will show them both to reveal these differences and strengthen the reliability of the measurements. Cronbach's Alpha and the Composite Reliability are generally accepted above 0.7 (Hair et al., 2011). To determine the validity, first the convergent validity using the Average Variance Extracted (AVE) is conducted. Convergent validity refers to the degree of correlation among the construct items and validate that a factor is explained by the observed construct items (Higgins and Thompson, 1995). At least a value of 0.5 is required for sufficient convergent validity (Higgins and Thompson, 1995). Cronbach's Alpha, Composite Reliability and Average Variance Extracted (AVE) can be found in Table 2. Table 2 shows that all the requirements are met except Cronbach's Alpha value for the item SU.

Further data analysis was conducted to test the discriminant validity using the Fornell-Larcker Criterion (Fornell and Larcker, 1981) which refers to the extent to which of the construct's items correlate with only one construct (Henseler et al., 2009). The square root of each construct's AVE should be greater than the correlations with other constructs. Table 3 shows these values, where the squared root is in bold. Additionally, Cross Loadings analysis was conducted where each construct item should have greater value than all of its cross loadings (Chin, 1998). Results obtained show that the criteria for Cronbach's Alpha, Composite Reliability, Average Variance Extracted, Fornell-Larcker criterion and Cross Loadings are met and hence all proposed constructs and items can be considered as acceptable instruments for this research (Fornell and Larcker, 1981).

6.3. Model predictability and statistical significance

The proposed model assumes that a number of factors can predict behavioural intention to use IoT devices at the workplace. These factors are: perceived usefulness, ethics of use, trust, concerns for information privacy (concerns regarding errors in collected information, secondary purpose of use, improper access and collection). The relationships explaining how the influencing factors predict BI are modelled using Partial Least Square (PLS) regression. The coefficient of determination (R-square), which measures the variance in the endogenous variable that is explained by the observed exogenous variables (Chin, 1998), will be used to test the model prediction accuracy. For that, SmartPLS was used to build the PLS regression. According to Chin (1998), the values of R-square are 0.67 for substantial, 0.33 for moderate and 0.19 for weak path models. The usual way to calculate the R-square for each dependent variable is by using the formula:

$$R^2 = 1 - \frac{\sum_{i=1}^{n}(X_i - Y_i)^2}{\sum_{i=1}^{n}(X_i - \bar{X})^2} \quad (8)$$

where Y_i represents the predicted value, X_i represents the actual values, and $\bar{X}$ is the mean.

In this study, the variance of BI has been calculated by taking into account the combined effect of the various predictors. An R-square value of 0.388 was found for BI. This means that the variables risk, trust, ethics, perceived usefulness and concerns for information privacy explain 39% of the variances in the output BI which can be considered as moderate. The other variables are shown to have a weak path model. The next step includes evaluating the path coefficients of the structural model, which can be found in Fig. 2. These are also known as regression weights. According to Cohen (1988), the effects of the path are considered to be 0.02 for small, 0.15 for medium and 0.35 for large. In this model perceived usefulness (0.447) has a large effect on behavioural intention, and concerns for errors (0.161) has a medium effect on behavioural intention. Looking at the other variables, risk has a medium effect on concern for improper access (0.266), collection (0.173), errors (0.307) and secondary use (0.304).

Table 4 shows the Pearson correlation coefficient (r) values at 95% confidence levels. In this study, it was found that perceived usefulness, Ethics and Trust showed statistically significant positive relationship with behaviour intention. Concerns regarding errors showed weak positive correlation which is not statistically significant. Concerns regarding secondary use, data collection and improper access scored negative correlation values which are not statistically significant. A bootstrap procedure in SmartPLS has been performed to study the statistical significance of various path coefficients. The paths coefficients are considered statistically significant if the *t*-statistics give a value above 1.96. The following paths are found statistically significant: PU → BI, Col → Trust, IA → Trust, Risk → Err, Risk → SU and Risk → IA. The other paths scored below the t-statistic score 1.96 and are considered as not statistically significant.

Table 2
Cronbach's alpha, Composite Reliability and Average Variance Extracted.

Constructs	Cronbach's Alpha > 0.7	Composite Reliability > 0.7	Average Variance Extracted > 0.5
Concern for information privacy (COL)	0.929	0.949	0.822
Concern for information privacy (ERR)	0.853	0.898	0.692
Concern for information privacy (IA)	0.750	0.855	0.667
Concern for information privacy (SU)	0.558	0.818	0.692
Ethics (ETHICS)	0.761	0.857	0.669
Trust (TRU)	0.944	0.956	0.784
Risk (RSK)	0.852	0.900	0.692
Perceived usefulness (PU)	0.963	0.967	0.746
Behavioural intention (BI)	0.946	0.959	0.823

Table 3
Fornell-Larcker Criterion.

Fornell-Larcker Criterion	BI	COL	ERR	Ethics	IA	PU	Risk	SU	Trust
BI	**0.907**								
COL	−0.199	**0.906**							
ERR	0.203	−0.049	**0.832**						
Ethics	0.278	−0.277	0.075	**0.818**					
IA	0.010	0.051	0.365	−0.189	**0.817**				
PU	0.578	−0.138	0.156	0.242	0.016	**0.864**			
Risk	−0.342	0.274	0.182	−0.516	0.298	−0.397	**0.832**		
SU	−0.254	0.195	0.146	−0.157	0.137	−0.252	0.307	**0.832**	
Trust	0.347	−0.443	0.050	0.479	−0.203	0.420	−0.554	−0.079	**0.885**

The square root of each construct's AVE.

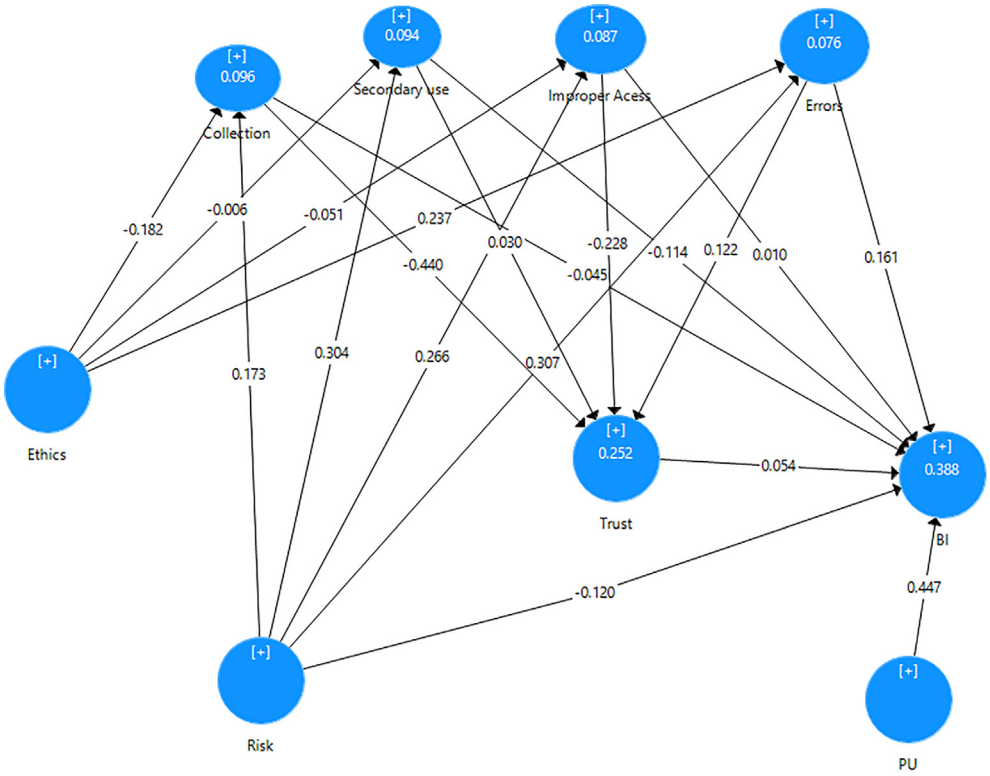

Fig. 2. Visual Illustration of the Relationship Model with Path Coefficients.

Table 4
Pearson Coefficient Correlation with Behavioural intention (BI).

	PU	ETHICS	RISK	TRUST	IA	SU	ERR	COL
r	0.558	0.287	−0.150	0.340	−0.042	−0.221	0.153	−0.217
P-value	0.0	0.012	0.196	0.003	0.718	0.055	0.0551	0.187

95% confidence level – two tailed.

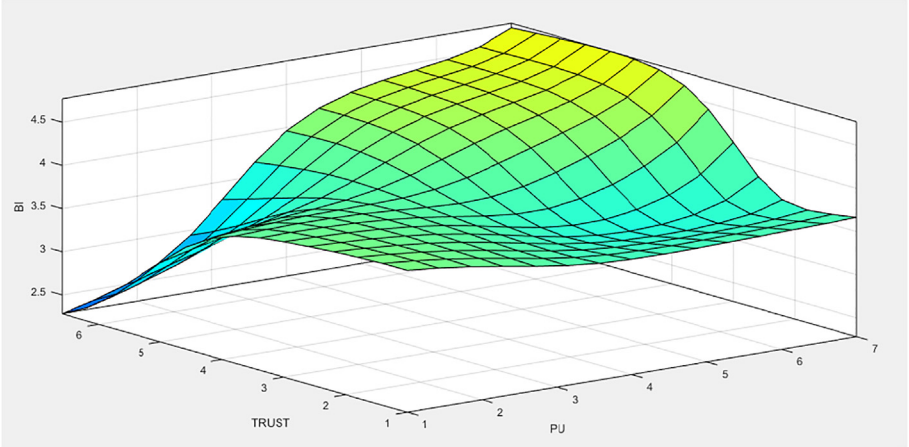

Fig. 3. Visual Illustration of Effect of Trust and PU on BI.

6.4. Using ANFIS

In this section, the properties of the ANFIS system that was generated for this study are shown. Matlab automatically generated membership functions type and parameters that suits the dataset. For each input variable, the Gaussian membership function was selected. By using the training functionality in the ANFIS model, the fuzzy output is fine-tuned to meet the dataset pattern. The more data fed to the model, the more accurate it becomes to predict BI. The fuzzy system generated rules automatically. Fig. 3 shows that the higher the trust values, the higher the impact of PU on BI starting from PU = 3.

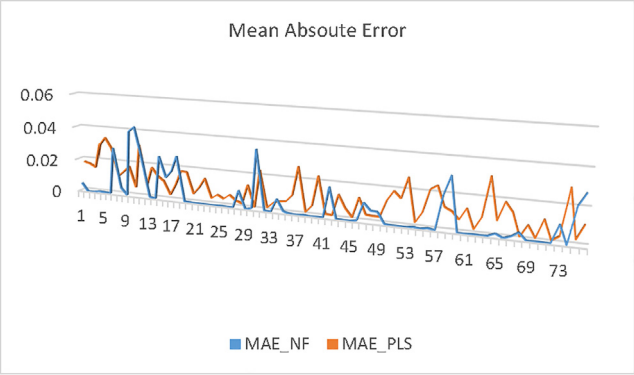

Fig. 4. Mean Absolute Error of PLS vs ANFIS for 76 users.

Fig. 4 shows mean absolute error (MAE) of the neuro-fuzzy system compared to the partial least square method for the 76 participants. It was noticed that the neuro-fuzzy has an overall MAE of 0.46 compared to PLS which scored MAE of 0.84. Besides, and by using Weka data mining toolkit (Smith and Frank, 2016), both algorithms recorded less error than different machine learning algorithms such as the improved sequential minimal optimisation (SMO) algorithm (Shevade et al., 2000) (MAE = 1.14) and the multilayer perceptron approach (MAE = 1.5). By calculating R-Square, it was found that the applying the neuro-fuzzy approach on the model has improved the predictability of BI from 0.39 to 0.64.

6.5. Precision and recall analysis

Performance of the neuro-fuzzy and the PLS models was evaluated using a precision and recall analysis (Stehman, 1997). As previously mentioned, behaviour intention values range from 1 to 7 and can be summarized in two categories; willing to use IoT devices (BI $\geq$ 3.5) and not willing to use IoT devices (BI < 3.5). The confusion matrix is shown in Table 5 while precision and recall analysis parameters are shown in Table 6. From this analysis, it can be seen that both data analysis methods showed good results where the performance of the neuro-fuzzy outperforms that of the PLS algorithm.

7. Discussion

This study attempted to identify the factors that influence an individual's behavioural intention (BI) to use an IOT wearable device at the workplace. The reliability and validity of the proposed model and relationships were tested using the partial least square path modelling and the ANFIS approaches. The results presented in the previous section displayed a moderate R-square value of 39% with regards to the behavioural intention of using a wearable device at the workplace, which is common in studies that attempt to predict human behaviour (Macdonell, 2010). We noticed that after applying the ANFIS model, the proposed model predictability increased to 64%.

The path coefficients related to privacy concerns, ERR → BI, SU → BI, IA → BI, Col → BI, which are depicted in Fig. 2, include two negative path coefficients. The negative path coefficient, Col → BI, indicates that higher levels of concerns regarding collection correspond to lower values for the behavioural intention of using a wearable device. This is because individuals are concerned that companies collect too much sensitive information. This negative effect on the behavioural intention of individuals confirms findings in (Dinev and Hart, 2006; Malhotra et al., 2004). In addition, the path coefficient of −0.045 is, according to Cohen (1988), considered small, which means that, in this study, the privacy concern regarding collection did not have a real effect on the behavioural intention of using a wearable device at the workplace. Secondly, the negative coefficient for SU → BI means that higher levels of individuals' concerns regarding unauthorized secondary use lead to lower levels of behavioural intention. Individuals are concerned that personal information might be used for purposes other than those mentioned. This finding goes in line with findings in (Dinev and Hart, 2006; Malhotra et al., 2004). The positive path coefficient Err → BI means that concerns regarding errors or lack of accurate data about users do not negatively influence the behavioural intention of using a wearable device as this reduces their concerns on privacy. The path coefficient of improper access and behavioural intention was 0.010, which can be ignored.

Although it was expected that the concerns individuals have regarding privacy would affect their behavioural intention of using wearable devices at the workplace, the results in this study indicate that it is not one of people's main considerations when it comes to using these devices at work. One of the main reasons that this concern did not affect the behavioural intention could be because people tend to be less conservative with regards to their privacy when they are at work. This conclusion confirms the result of a study on the usage of location based services by Ali Eldin (2006). Another reason is that the majority of participants were males (88%) who are generally less concerned about privacy than female participants which goes in line with the results of Zukowski and Brown (2007). Nevertheless, using IoT wearable devices in different contexts such as healthcare can raise more concerns on users' privacy (Yiwen et al., 2015).

It was noticed that concerns regarding collection and improper access have a negative impact on perceived trust. This means that individuals with high levels of concerns regarding collection of information and improper access to the collected data show little trust in the employer offering wearable technology. However, concerns regarding errors (data accuracy) does not affect individuals'

Table 5
Confusion Matrix.

		Algorithm	Actual BI of 76 users	
			Willing to use IOT (45)	Not willing to use IOT (31)
Predicted BI	Willing	ANFIS	41 True Positive (TP)	5 False Positive (FP)
	Not willing		4 False Negative (FN)	26 True Negative (TN)
	Willing	PLS	33 True Positive (TP)	8 False Positive (FP)
	Not willing		12 False Negative (FN)	23 True Negative (TN)

Table 6
Precision and Recall Analysis.

	Precision	Recall	F-score	TPR	TNR	PPV	NPV	FNR	FPR	FDR	FOR	ACC.
ANFIS	0.89	0.91	0.91	0.91	0.84	0.89	0.87	0.09	0.16	0.11	0.13	0.88
PLS	0.81	0.73	0.77	0.73	0.74	0.81	0.66	0.27	0.26	0.20	0.35	0.74

trust towards their employer. It has a small positive impact on trust, which means despite the higher the concern regarding data accuracy, the confidence in the company remains. The path between concerns regarding unauthorized secondary use and trust has a path coefficient of 0.030, which is very close to zero. It can be concluded that, in this study, unauthorized secondary use concerns had no effect on perceived trust.

Individuals who believe that companies are trustworthy when it comes to handling information demonstrate a higher behavioural intention of using a wearable device. It seems obvious that increasing trust will result in an increased likelihood of an employee using a wearable device. Studies that have investigated trust in general and its effect on behavioural intention confirm that it indeed can have a positive effect on behavioural intention (Gefen, 2000; Morawczynski and Miscione, 2008) but in another study on trust impact on consumer behaviour by (Dierks, 2007), it was found that effect of trust was considerably low in normal or safe contexts. In this study, trust was found to play an intermediate role between behaviour intention and some concerns for information privacy (improper access and information collection) which is close to findings obtained by Esmaili et al. (2011). Further, trust was found to have rather weak positive correlation (0.33) which is statistically significant. However, results from the PLS regression show that the path trust → BI is rather weak and trust is not an important predictor of BI in this study. This results confirms the findings of (Dierks, 2007) that trust plays a marginal effect on consumer behaviour in normal and safe contexts but in critical situations, such as food or healthcare related, its effect will become important.

Individuals who believe that it would be risky to use a wearable device have high privacy concerns regarding collection, errors, secondary use and improper access. Individuals who consider wearable devices risky or unsafe have a low behavioural intention of using them. Risk determines intention, and as the risk increases, the behavioural intention of using a wearable decreases. Previous research confirms that reducing risk strongly affects the behavioural intention of using a technology (Chen, 2008). In this study, risk was found to have a medium negative effect on behaviour intention which is not statistically significant. Risk influence was not found high enough as expected because participants in the survey are already familiar with the technology and can behave similar to actual users and not potential users. Usually potential users of a technology would have more uncertainties around the use of such new technology leading to financial, performance and privacy risks as was concluded by Yang et al. (2016).

Individuals who find the wearable device useful in their job have a greater tendency to use a wearable device. In this study, perceived usefulness, which originates from the TAM (Davis et al., 1989), is the most important variable in influencing behavioural intention to use IoT devices at work. People have a higher likelihood of using a wearable device when they find the device useful and likely to improve their performance. This study confirms the conclusion of Venkatesh and Davis (2000) that it has a positive effect on behavioural intention. The results of this study indicate that individuals who have greater interest in obtaining services or information have fewer privacy concerns regarding collection, unauthorized secondary use and improper access.

Overall, the t-statistics of the variables in this study, which indicate the certainty of a difference or connection, were considerably low. These relationships could be identified if a larger study were to be conducted. Previous research proved that these variables are important in determining the behavioural intention of individuals (Fishbein and Ajzen, 1975; Malhotra et al., 2004); however, in this study, there was little significant effect. This does not mean that these variables are not important as it is possible that further research with a different or larger population could produce a significant result.

8. Conclusion

The main dependent variable or output in this study is the behavioural intention of an individual to use IoT wearable devices at the workplace and the aim of this study was to identify which factors can predict this dependent variable. The results indicate that 39% of the variance in the output can be accounted for the factors in the conceptual model proposed in this study. It was shown that this percentage could be improved using the ANFIS approach. Further in this study, perceived usefulness had strong significant positive relationship with behaviour intention. The individuals, surveyed in this study, are more likely to use a wearable device at the workplace once they believe that it will improve their performance and increase their productivity.

This study did not find statistically significant relationship between privacy concerns and behaviour intention of using a wearable device at work. Additionally, it was not found that perceived risk can significantly predict behavioural intention. Besides, trust and concerns regarding ethics were found to have statistically significant positive relationship with behaviour intention but is rather weak. Further, trust was not found to be an important predictor of behaviour intention in this study. This shows the complexity in the relationships amongst the different factors being studied. This result can firstly be explained by the fact that this study was amongst ICT professionals who can be considered as actual users and not really potential users. Besides, the study was not on specific wearable devices nor focused on certain critical domains like healthcare but rather on a less privacy sensitive context which is the workplace. Furthermore, majority of the respondents showed positive intention to use the devices and perceived these devices as useful at work.

Perceived usefulness was found to be an important predictor of behavioural intention. It was found that a significant relationship between some privacy concerns and trust exists. In addition, significant relationship between risk and some privacy concerns was found meaning that individuals' with high perceived risk towards the use of wearable devices would have high privacy concerns.

There are several opportunities for further research. The population of this study showed many similarities in gender, age, education and nationality. More specifically, the participants were mainly educated males from the Netherlands. It is therefore possible that a study with another sample will present different findings, for example when looking at different cultures. As this study was conducted within a specific organization, further studies should be conducted at different organizations before one can generalize the results obtained in this paper. Besides, future research could examine the perspectives of different cultures, corporate and societal, and involve a greater number of respondents. Future research could also perform multi-group analyses to examine whether the control variables have effects on the path of the model.

Acknowledgement

The authors would like to acknowledge that the work in this paper was conducted partially at CGI Nederland as an internship project in the period May-October 2016.

References

Abdolmohammadi, M.J., Baker, C.R., 2006. Accountants' value preferences and moral reasoning. J. Business Ethics 69, 11–25.

Ajzen, I., 1985. From intentions to actions: A theory of planned behavior. In: Beckman, J.K.J. (Ed.), Action-control: From cognition to behavior. Springer, Heidelberg.

Ali Eldin, A. and R. Wagenaar. A Fuzzy Logic based Approach to support users self-control of their private contextual data retrieval. in 12th European Conference on Information Systems (ECIS04). 2004. Turku, Finland.
Ali Eldin, A., van den Berg, J., Wagenaar, R., 2004. A Fuzzy reasoning scheme for context sharing decision making. 6th International Conference on Electronic Commerce. ACM Press, Delft, The Netherlands.
Ali Eldin, A., Wagenaar, R., 2007. Towards Autonomous User Privacy Control. Int. J. Inf. Security Privacy 1 (4), 24–46.
Ali Eldin, A., Private Information Sharing Under Uncertainty. 2006, Delft: Copy Right (C) Amr Ali Eldin. 160.
Aquino, Karl, 1998. The effects of ethical climate and the availability of alternatives on the use of deception during negotiation. Int. J. Conf. Manage. 9 (3), 195–217.
Bansal, G., F. Zahedi, and D. Gefen, The Moderating Influence of Privacy Concern on the Efficacy of Privacy Assurance Mechanisms for Building Trust: A Multiple-Context Investigation. ICIS 2008 Proceedings., 2008.
Bauer, R.A., 1967. Consumer Behaviour as Risk Taking. In: Cox, D.F. (Ed.), Risk Taking and Information Handling in Consumer Behaviour. Harvard University Press.
Campbell, A.J.J., 1997. Relationship marketing in consumer markets: a comparison of managerial and consumer attitudes about information privacy. Direct Market. 11 (3), 44–57.
Chen, H., 2008. Individual Mobile Communications Services and Tariffs. Erasmus Research Institute of Management (ERIM). Erasmus University Rotterdam, Rotterdam, the Netherlands.
Chin, W.W., The partial least squares approach to structural equation modeling. Modern methods for business research ed. G.A. Marcoulides. 1998, Mahwah, NJ.: Lawrence Erlbaum.
Cho, H., Rivera-Sánchez, Milagros, Lim, S.S., 2009. A multinational study on online privacy: global concerns and local responses. New Media Soc. 11 (3), 395–416.
Clarke, R., 1999. Internet privacy concerns confirm the case for intervention. Commun. ACM 42 (2), 60–67.
Cohen, J., Statistical power analysis for the behavioral sciences. 1988, Hillsdale N.J.: L.Erlbaum Associates.
Cole, B.C., Smith, D.L., 1996. Perceptions of business ethics: students vs business school students. J. Business Ethics 13, 693–700.
Cronbach, L.J., 1951. Coefficient alpha and the internal structure of tests. Psychometrika 16, 297–334.
Cunningham, S.M., 1964. Perceived risk as a factor in product-oriented word-of-mouth behavior: A first step. In: Smith, L.G. (Ed.), Reflections on Progress in Marketing. American Marketing Association, Chicago.
Davis, F.D., 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quart. 13 (3), 319–340.
Davis, F.D., Bagozzi, R.P., Warshaw, P.R., 1989. User acceptance of computer technology: a comparison of two theoretical models. Manage. Sci.
Dierks, L.H., 2007. Does trust influence consumer behaviour? Beeinflusst Vertrauen das Verbraucherverhalten? Agrarwirtschaft 56 (2).
Dillon, A. and M. Morris, User acceptance of new information technology: theories and models.. Annual Review of Information Science and Technology, ed. M. Williams. 1996.
Dinev, T., Xu, H., Smith, J., Hart, P., 2013. Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. Eur. J. Inf. Syst. 22, 295–316.
Dinev, T., Hart, P., 2006. An extended privacy calculus model for E-commerce transactions. Inf. Syst. Res.
Elaklouk, A.M., Zin, N.A.M., Shapii, A., 2015. Investigating therapists' intention to use serious games for acquired brain injury cognitive rehabilitation. J. King Saud Univ. – Comput. Inf. Sci. 27 (2), 160–169.
Esmaili, E., Desa, M.I., Moradi, H., Hemmati, A., 2011. The role of trust and other behavioral intention determinants on intention toward using internet banking. Int. J. Innovation, Manage. Technol. 2 (1).
Fishbein, M., Ajzen, I., 1975. Belief, Attitude, Intention and Behaviour: An Introduction to Theory and Research. Addison-Wesley, Pub., p. 578.
Flaherty, J.L., 2014. Digital diagnosis: privacy and the regulation of mobile phone health applications. Am. J. Law Med. 40 (4), 416–441.
Fornell, C., Larcker, D.F., 1981. Evaluating structural equation models with unobservable variables and measurement error. J. Market. Res. (JMR) 18 (1), 39–50.
Fried, C., 1970. An Anatomy of Values: Problems of Personal and Social Choice. Mass: Harvard University Press, Cambridge.
Gartner Gartner Says Worldwide Wearable Devices Sales to Grow 18.4 Percent in 2016. Retrieved from Gartner: *http://www.gartner.com/newsroom/id/3198018* - Last visited on 16 June 2016. 2016.
Gartner Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015 retrieved from: *http://www.gartner.com/newsroom/id/3165317* - Last visited on 16 June 2016. 2015.
Gefen, D., 2000. E-commerce: the role of familiarity and trust. Omega. Int. J. Manage. Sci. 28 (5), 725–737.
Gefen, D., Karahanna, E., Straub, D.W., 2003. Trust and TAM in online shopping: an integrated model. MIS Quart. 27 (1), 51–90.
Graeff, T.R., Harmon, S., 2002. Collecting and using personal data: consumers' awareness and concerns. J. Consumer Market.
Hair, J.F., Ringle, C.M., Sarstedt, M., 2011. PLS-SEM: indeed a silver bullet. J. Market. Theory. Practice 19 (2), 139–151.
Hamblen, M., As smartwatches gain traction, personal data privacy worries mount: companies could use wearables to track employees' fitness, or even their whereabouts, in Computerworld. 2015.
Henseler, J., Ringle, C.M., Sinkovics, R.R., 2009. The use of partial least squares path modeling in international marketing. Adv. Int. Market.
Higgins, D.B., Thompson, R., 1995. The partial least squares (PLS) approach to causal modeling: personal computer adoption and use as an illustration. Technol. Studies.
Jang, J.S.R., 1993. ANFIS: adaptive-network-based fuzzy inference system. IEEE Trans. Syst., Man, Cybernetics 23 (3), 665–685.
Jarvenpaa, S.L., Tractinsky, N., 1999. Consumer trust in an internet store: a cross-cultural validation. J. Comput.- Mediated Commun. 5 (2).
Lifton, P., 1985. Individual differences in moral development: the relation of sex, gender, and personality to morality. J. Personality.
Liu, C., Marchewka, J.T., Lu, J., Yu, C.S., 2005. Beyond concern-a privacy-trust-behavioral intention model of electronic commerce. Inf. Manage. 42, 289–304.
Macdonell, K. How high, r-squared? Retrieved from https://cooldata.wordpress.com/2010/04/19/how-high-r-squared/ - Last visited on 29 Aug. 2016. 2010.
Malhotra, N.K., Kim, S.S., Agarwal, J., 2004. Internet User' Information Privacy Concerns (IUIPC): the construct, the scale, and a causal model. Inf. Syst. Res. 15 (4), 336–355.
Mason, R.O., 1986. Four ethical issues of the information age. Manage. Inf. Syst. Quart. 10 (1).
Mayer, R.C., Davis, J.H., Schoorman, F.D., 1995. An integrative model of organizational trust. Acad. Manage. Rev.
miCoach, Retrieved from http://micoach.adidas.com/ - Last visited on 20 July 2016. 2015.
Morawczynski, O. and G. Miscione, Exploring trust in mobile banking transactions: the case of M-Pesa in Kenya. Retrieved from https://www.microlinks.org/library/exploring-trust-mobile-banking-transactions-case-m-pesa-kenya. Last visited on 26 Nov. 2016. 2008.
Morris., R. Wearable Technology. Function, Fit, Fashion, Retrieved from *http://www.onebeacontech.com/Technology/pages/news/detail/whitepaper.page?id=d537ede26772af84785f5a19ffb5be56* - Last visited on 30 June 2016. 2015.
Mowen, J.C., 1992. The time and outcome valuation model: implications for understanding reactance and risky choices in consumer decision-making. Adv. Consumer Res.
Parent, W.A., 1983. Privacy, Morality, and the Law. Philosophy & Public Affairs 12 (4), 269–288.
Parker, R.B.D.o.p., A definition of privacy. Rutgers L. Reviews, 1973.
Peter, J.P., Ryan, Micheal J., 1976. An investigation of perceived risk at the brand level. J. Market. Res. 13 (4), 184–188.
Ringle, C.M., S. Wende, and J.-M. Becker "SmartPLS 3." Boenningstedt: SmartPLS GmbH, http://www.smartpls.com. Last visited on 12 Dec. 2016. 2015.
Schaninger, C.M., 1976. Perceived risk and personality. J. Consumer Res. 32 (2), 95–100.
Shevade, S.K., Keerthi, S.S., Bhattacharyya, C., Murthy, K.R.K., 2000. Improvements to the SMO algorithm for SVM regression. IEEE Trans. Neural Networks 11 (5), 1188–1193. https://doi.org/10.1109/72.870050.
Smith, T.C., Frank, E., 2016. Introducing Machine Learning Concepts with WEKA. In: M. E.,, D. S. (Eds.), Statistical Genomics. Methods in Molecular Biology. Springer, New York, pp. 353–378.
Smith, H.J., Milberg, S.J., Burke, S.J., 1996. Information privacy: measuring individuals concerns about organizational practices. MIS Quart. 20 (2), 167–196.
Stehman, S.V., 1997. Selecting and interpreting measures of thematic classification accuracy. Remote Sens. Environ. 62 (1), 77–89.
Stewart, K.A., Segars, A.H., 2002. An empirical examination of the concern for information privacy instrument. Inf. Syst. Res.
Taylor, J.W., 1974. The role of risk in consumer behaviour. J. Market. 38 (2), 54–60.
Tehrani, K. and A. Michael, Wearable technology and wearable devices: Everything you need to know. Wearable Devices Magazine, 2014.
Venkatesh, V., Morris, M.G., Davis, G.B., Davis, F.D., 2003. User acceptance of information technology: toward a unified view. MIS Quart.
Venkatesh, V., Davis, F.D., 2000. A theoretical extension of the technology acceptance model: four longitudinal field studies. Manage. Sci. 46 (2), 186–204.
Warren, S., Brandeis, D., 1890. The right to privacy. Harv. Law Rev. 4 (5), 193–220.
A. Westin, Privacy and freedom, New York, 1968, U.S.A Atheneu.
Yang, H., Yu, J., Zo, H., Choi, M., 2016. User acceptance of wearable devices: an extended perspective of perceived value. Telematics Inf. 33 (2), 256–269. https://doi.org/10.1016/j.tele.2015.08.007.
Yi, M.Y., Jackson, J.D, Park, J.S., Probst, J.C., 2006. Understanding informationtechnology acceptance by individualprofessionals: toward an integrative view. Inf. Manage. 43, 350–363.
Yiwen, G., He, L., Yan, L., 2015. An empirical study of wearable technology acceptance in healthcare. Indust. Manage. Data Syst. 115 (9), 1704–1723.
Yu-Hui, C., Stuart, B., 2007. Initial trust and online buyer behaviour. Indust. Manage. Data Syst. 107 (1), 21–36.
Zukowski, T. and I. Brown, Examining the Influence of Demographic Factors on Internet Users' Information Privacy Concerns, in the 2007 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries. 2007. p. 197-204