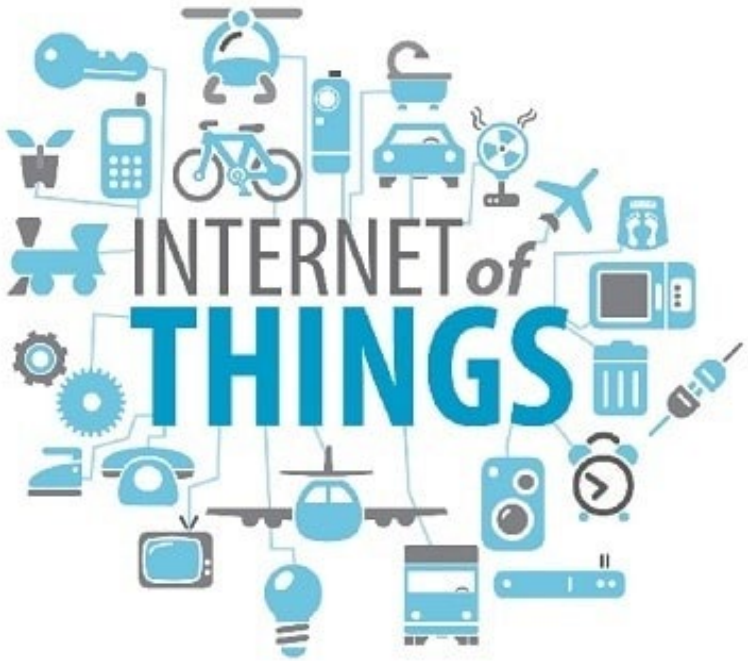
Internet of Things: The effect of perceived privacy and perceived benefits on acceptance



Author: K. van ‘t Wel

Student number: 971205937130

Supervisor: dr. A.M. Griffioen

2nd reader: dr.ir. A.R.H. Fischer

Course code: YSS- 81812

Wageningen University and Research

22th of January 2019

Picture: RF page/ Specifications and Applications of Narrow Band IoT (NB-IoT)

Abstract

This study aims to research to what extent perceived privacy revelation and the degree of perceived benefits affect the acceptance of Internet of Things (IoT) applications. To research this question a new conceptual model has been created on the basis of TAM, UTAUT, equity theory and the privacy calculus theory. In a thought experiment, participants were randomly assigned to a 2 (Privacy revelation: low/high) x 2 (Benefits: low/high) between-subjects design and were asked whether they would accept a particular IoT application (i.e., Home Assistant). Besides, the level of trust in IoT applications has been measured before the manipulation took place. This study expected that a high level of benefits and a high level of trust would increase the acceptance and a high level of privacy revelation would decrease the acceptance. The main findings of this study are that the degree of perceived benefits has an effect on the acceptance of IoT applications and perceived privacy revelation has not an effect on the acceptance of IoT applications. Further, the level of trust in IoT applications has a positive effect on the acceptance of IoT applications. Accordingly, companies creating and selling IoT applications should ensure that the benefits of their applications are high and that the applications and the company itself are perceived as trustworthy by the consumers.

Content

1. INTRODUCTION

Suppose you are searching for a new coffee machine. There is a new high-tech coffee machine which gives a notification, via the email of the company, if it needs maintenance and when they have personalised offers on the basis of your coffee-making frequency. Would you accept this new technology?

In this case there is a trade-off between the revelation of privacy sensitive information and the benefits of the service/product. This kind of applications are feasible through the use of the technology named the Internet of Things. Currently, there is little research that focuses on the trade-off between the revelation of privacy sensitive information and the benefits of such applications and its resulting effect on the acceptance of the Internet of Things. Therefore, this research aims to address this issue by studying if there are any relations between the amount of revealed privacy, the additional benefits and the acceptance of Internet of Things applications.

1.1 The Internet of Things

The Internet of Things (IoT), is a network of smart devices equipped with sensors and radio-frequency identification, connected to the internet. The smart devices are able to share information with each other, without human intervention (Pretz, 2013).

The IoT is an increasing industry with rapid developments. The IoT is a new revolution of the Internet. Objects and products have unique identifiers and are able to communicate with each other. They obtain intelligence by making or enabling context related decisions thanks to the fact that they can communicate information about themselves (Vermesan & Friess, 2013). This gives the opportunity to create applications, which make decisions and perform activities, in service of the user. In return, the user of the application has to give up privacy sensitive information, which the application uses to make decisions and perform activities.

These applications are being adopted in a wide variety of environments. These environments are often divided into the following parts: smart health, smart cities, smart energy, smart transport, smart living and smart buildings.

1.2 Research aim

This study will research if there is a relation between three different aspects: the privacy revelation with the use of IoT applications (privacy), the benefits with the use of IoT applications (benefits) and the acceptance of IoT applications (acceptance). It has been found that consumers sacrifice a certain portion of their privacy in lieu of some benefits consisting of financial incentives or convenience (Hann, Hui, Tom Lee, & Ivan, 2007). Privacy and benefits can be related to each other with the use of the equity theory. In the equity theory, equity is measured by comparing the ratio of contributions (or costs) and benefits (or rewards) for each person (Guerrero, A. Andersen, & Afifi, 2014). Subsequently, there may be a positive or negative effect on the acceptance of IoT applications. Numerous theories about technology acceptance have been developed overtime, such as the Technology Acceptance Model (TAM; Davis, Bagozzi, & Warshaw, 1989) and the Unified Theory of Acceptance and Use of Technology (UTAUT; Venkatesh, Morris, Davis, & Davis, 2003). Nevertheless, the connection between the amount of perceived privacy revelation, perceived benefits and the acceptance of IoT applications has not been researched with these or other theories yet.

Therefore, the following research question has been formulated:
To what extent have perceived privacy revelation and the degree of perceived benefits effect on the acceptance of Internet of Things applications?

In order to answer the research question, the following sub-questions have been formulated:

- What is the effect of a high amount of perceived privacy revelation in combination with a high/low amount of perceived benefits on the acceptance of Internet of Things applications?
- What is the effect of trust on the relationship between the acceptance of Internet of Things applications and the privacy-benefit trade-off?

1.3 Relevance of the research

The study will have a substantial and original contribution to the already existing literature around technology acceptance and trade-offs being made between privacy and benefits. Revenue models are becoming more and more based on data driven decision making. Data driven decision making means that companies make decision on the basis of verifiable data rather than making decisions intuitively, in order to enhance their revenues. For example, on the basis of the daily food consumption of a customer, supermarkets can make some personal offers. IoT applications are an appropriate way to generate these data for decision making. Companies like KPN are already using IoT applications in their revenue models and more companies will follow. Therefore, this study will be of interest for companies using IoT to support their businesses and companies which have based or are going to base their business and revenue model on IoT. The outcomes of the study will help marketers and researchers to understand the extent to which consumers are willing to give up their privacy for the resulting benefits and the effect of this trade-off on the acceptance of IoT applications. This can be used by marketers to better respond to the consumer and offer services and products which better match with the thoughts and behaviours of consumers.

1.4 Structure

This study will be a quantitative study which consists out of 5 chapters. After the introduction there will be the theoretical framework. The theoretical framework discusses the theoretical constructs and models. In addition, relevant factors related to these theories will be discussed. In the research design the methodology of the research will be elaborated. In the research results section, the outcomes of the study will be discussed and explained. The discussion contains the conclusions that can be drawn on the basis of the study, the restrictions of the study and suggestions for further research.

2. Theoretical Framework

2.1 Perceived benefits

With the use of IoT applications life can become easier. For example: remote control appliances, appliances can be switched off and on automatically to avoid accidents and save energy (Patel & Patel, 2016). There has been a lot of research on the acceptance of such technology driven products in the past. Two theories have been widely used in research on technology acceptance, namely the Technology Acceptance Model (TAM; Davis, Bagozzi, & Warshaw, 1989) and the Unified Theory of Acceptance and Use of Technology (UTAUT; Venkatesh, Morris, Davis, & Davis, 2003).

The UTAUT includes four constructs that play a role as determinants of user acceptance and user behaviour: performance expectancy, effort expectancy, social influence and facilitating conditions. Next to this, the UTAUT includes four moderators: gender, age, experience and voluntariness of use (Venkatesh et al., 2003). However, not all of the variables in UTAUT are always significantly influencing the behavioural intention to adopt technology. For example, in a study on the behavioural intention to adopt IoT in the contexts of a smart city, a number of factors (security risks, social influence, facilitating conditions and habit) were not significantly influencing the intention to adopt IoT (Leong, Ping, & Muthuveloo, 2017).

In an earlier study, UTAUT has been proven to be more powerful than TAM in the ability to explain the variances in the acceptance of technology (Al-Momani, Mahmoud, & Ahmad, 2016). Nevertheless, has TAM been used is several studies. TAM is an adaption on the theory of reasoned action (TRA), and has been used to model the acceptance of technology and information systems (Davis et al., 1989). There are two variables being used in TAM to predict the acceptance of technology based products. The two proposed relevant variables for predicting the acceptance of technology based products are, Perceived Usefulness (PU) and Perceived Ease of Use (PEU). Perceived Usefulness has been defined as the users' subjective probability that using a specific applications (e.g., IoT application) will increase his or her performance and Perceived Ease of Use has been defined as the degree to which the user expects the application to be effortless (Davis et al., 1989).

In different contexts, different variables may be influencing the behavioural intention to adopt a technology. Therefore, this study will use findings from TAM and UTAUT and incorporate the relevant factors for the acceptance of IoT applications. These relevant factors are perceived benefits, perceived privacy and trust, and will be elaborated upon in section 2.1, 2.2 and 2.4. In this way the study is based on a solid foundation.

In a previous study on the factors influencing the acceptance of IoT, perceived usefulness was similar to performance expectancy of the UTAUT and perceived ease of use was similar to the effort expectancy of the UTAUT (Gao & Bai, 2014). Previous work has shown that usefulness is the most powerful predictor and followed by the ease of use, trust and enjoyment (Davis et al., 1989; Gao & Bai, 2014). Hence, this study will use usefulness and ease of use to determine the perceived benefits of the consumer. With respect to the factor perceived benefits, the following hypothesis has been made:

H1. Higher Perceived Benefits will have a positive effect on the acceptance of IoT applications.

2.2 Perceived privacy

In non-electronic environments, there is little privacy sensitive information being tracked and stored. In the time that there was no internet, loss of privacy information was already there. For example, financial information like bank statements or personal information stated on passports were

stolen by thieves. With the advent of Big Data and IoT, personal information is being exposed more widely (Adams, 2017). Within the IoT-based environment, a wide variety of applications monitor and record information about consumer behaviour in daily life (Weinberg, Milne, Andonova, & Hajjat, 2015). For example, the types of coffee someone makes every morning. In return the consumer may receive a discount on the type of coffee he or she makes. In other words, through time more personal information is being monitored and relevant benefits may come with this trend. Therefore, it is important to investigate the amount of personal information a consumer is willing to disclose for the benefits of IoT applications. Since this trade-off may affect the acceptance of such applications. In order to research this, several factors have to be distinguished. This study distinguishes the following factors: types of personal information and the amount of revelation.

Types of personal information

Different types of information are being monitored by IoT applications. Consumers may have different thoughts about the revelation of different kind of personal information. As mentioned before, IoT applications are being adopted in a wide variety of environments. In these environments, various personal information is needed by IoT applications to operate. In the health sector, IoT applications can be used to monitor personal vital functions such as: temperature, blood pressure, heart rate and stimulate the heart muscles in case of a heart attack (Dlodlo, Foko, Mvelase, & Mathaba, 2012). All kind of personal body values can be monitored by wearable devices and other home sensing applications can be used to monitor the behaviour of people inside their home in order to support those people. In the environment of smart cities, there are several IoT applications. On the street, consumers can be monitored by cameras in order to support the police and the location of consumers' cars can be monitored in order to suggest the closest parking space or to manage the traffic in cities (Abaker Targio HAshem et al., 2016). In addition to the environments of smart health and smart cities, a lot of personal information is being monitored in smart homes. Depending on the application, the following kind of information can be monitored: energy usage, what consumers say, where consumers are, the contents of the refrigerator, activities being performed, and even sexual activity (Apthorpe, Reisman, Sundaresan, Narayanan, & Feamster, 2017). The environment of smart homes will be used in this study, since personal information is intensively being monitored in this environment as illustrated above. In addition, a reason to choose smart home appliances, is the applicability of these appliances for almost all of the consumers. Not everyone suffers from health problems and not everyone is able to drive a vehicle, but almost everyone is living in a home.

Amount of revelation

To research the trade-off between revelation of privacy sensitive information and benefits it is important to take the amount of revelation into account. By changing the amount of revelation, the effect on the thoughts of the consumer about the trade-off can be measured and the effect on the acceptance of IoT applications.

In previous studies, the impact of privacy benefits and risk on consumers' desire to use IoT technology has been investigated (Lee, Ha, Oh, & Park, 2018). Such that higher perceived privacy risk will lower the acceptance of IoT technology. These kind of studies used the privacy calculus theory, which claimed that the individuals' intention of disclosing personal information will depend on the perceived privacy risks and the anticipated benefits (Ku, Li, & Lee, 2018). The current study does not directly measure the perceived privacy risks, since this study aims to investigated how much privacy sensitive information people are willing to give up for the benefits of IoT applications. This study mainly focusses on the amount and type of information revelation. Even though it is not the central point of this research, respondents will be asked if they see any privacy risks with the use of IoT applications, as privacy risks have an important effect on the acceptance following the theory of privacy calculus (Culnan & Armstrong, 1999). With respect to the factor perceived privacy, the following hypothesis has been made:

H2. More revelation of personal information will have a negative effect on the acceptance of IoT applications.

2.3 Cost-benefit calculus

To research the trade-off between perceived privacy and perceived benefits, this study used a combination of the equity theory and the privacy calculus theory. The equity theory (Adams, 1963) is based on the idea that the perceived equity is based on the users' comparison between the ratio of outputs (benefits) and the ratio of inputs (costs). When the inputs are higher than the outputs, the perceived equity is low, and when the inputs are lower than the outputs, the perceived equity is high. This theory asserts that users are willing to share personal information when the perceived benefits of IoT applications are higher than the perceived revelation of information. Despite the fact that the equity theory is already more than fifty years old, it is still applied in research today (Poushneh, 2018).

Besides the equity theory, *the privacy calculus* also embraces the idea of consumers making decisions to disclose personal information on the basis of a cost-benefit calculation (Culnan & Armstrong, 1999). In this calculus, the perceived benefits and the perceived risks of a transaction are weighted. The intention to disclose personal information rises if the benefits outweigh the risk (Wilson & Valacich, 2012). The similarities between the equity theory and the privacy calculus are applicable in this research. In the privacy calculus theory, privacy risks with IoT are associated with the fear of unfair use of private information by organizations, like over tracking and unauthorised access of data. Examples of perceived benefits with IoT in the privacy calculus theory, are real time decision making and enhanced tracking (Majumdar & Bose, 2016). Both theories would predict that when the perceived benefits of the IoT application outweigh the associated costs, this will enhance the acceptance of IoT applications.

This study expects that a combination of low benefits and high privacy revelation has a negative effect on the acceptance. Furthermore, this study expects all the other combinations between high or low benefits and high or low privacy revelation to have a positive effect on the acceptance, with high benefits and low privacy revelation to have the largest positive effect. Since this study expects consumers to prefer high benefits over low benefits and low privacy revelation over high privacy revelation.

Table 1: The effects of different combinations of privacy revelation and benefits on the acceptance of IoT applications

	Low Privacy Revelation	High Privacy Revelation
Low Benefits	+	-
High Benefits	+ +	+

With respect to the trade-off between perceived privacy and perceived benefits, the following three hypotheses has been made:

H3a. If the benefits are high, the acceptance will be positively affected, regardless of the level of the privacy revelation.

H3b. A combination of low benefits and low privacy revelation will have a positive effect on the acceptance

H3c. A combination of low benefits and high privacy revelation will have a negative effect on the acceptance.

2.4 Trust

Besides perceived benefits and perceived privacy, this study expects trust to have a direct effect on the acceptance of IoT applications and a moderating effect on perceived benefits and perceived privacy. Next to this, this study expects trust to have a moderating effect on perceived usefulness (one of the determinants of perceived benefits; Gefen, Karahanna, & Straub, 2003). According to the Theory of Reasoned Action (TRA; Fishbein & Ajzen, 1975), users' belief affect their intention. This implicates that consumers' trust affects their behavioural intention. In the literature, trust has been described in several ways. According to some of the definitions described in the literature, trust means the belief of an entity in the reliability of another entity and the confidence and belief that another entity will act in a beneficial way (Grandison & Sloman, 2000; Hornby, Cowie, & Gimson, 1988; Xiu & Liu, 2005).

Direct effect of trust on acceptance

Trust has been proven to have a direct effect on the acceptance of IoT applications (AlHogail, 2018; Belanche, Casaló, & Flavián, 2012; Gao & Bai, 2014; Khan, Aalsalem, Quratulain, & Khan, 2016; Yildirim & Ali-Eldin, 2018). Next to this, trust has been a critical motivational factor for the adoption of technology (Gefen et al., 2003). Therefore, this study expects trust to have a positive effect on the acceptance of IoT applications. If the trust in a IoT application rises, the acceptance of the IoT application will also rise. With respect to the direct effect of trust, the following hypothesis has been made:

H5. Trust has a positive effect on the acceptance of IoT applications.

Effect of trust on perceived privacy

Earlier research has found that the success of IoT applications essentially depends on the perceptions of the consumer about the security of products and the level of their trust (Khan et al., 2016). Numerous models have been developed that include trust as an predicting factor on the adoption of technology (AlHogail, 2018; Belanche et al., 2012; Gefen et al., 2003). AlHogail (2018) developed a model including major factors affecting trust towards IoT technology. A part of the model of AlHogail is also applicable for this study, namely the part of security related factors. Security related factors are described as product or service security and perceived risks. These factors affect trust towards IoT technology and are in this way part of the trust in IoT Technology. When the product security is low and the perceived risks of a product are high, the trust in the technology is low. In this case, someone may be hesitant to share personal information (Milne, Pettinico, Hajjat, & Markos, 2017). In this way, the amount of information shared by the consumers may be influenced by the level of trust (product security and risks). The lower the trust, the more someone hesitates to share personal information. One of the factors in this study is the amount of revelation of personal information (perceived privacy). Since the amount of trust may have an influence on the amount of revelation of personal information as described above, this study expects trust to have a moderating effect on the amount of revelation of personal information

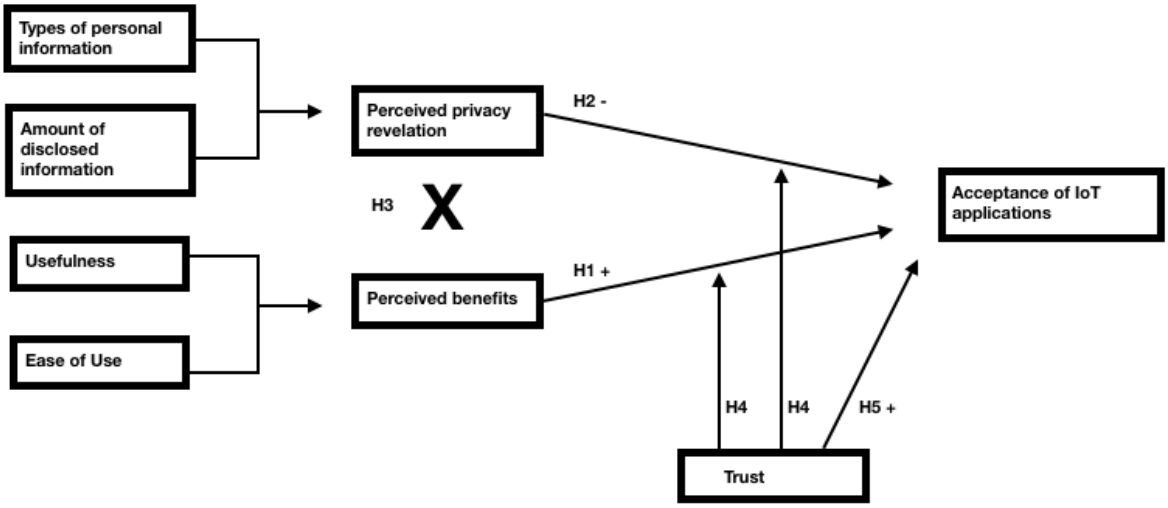
Effect of trust on perceived benefits

Besides the moderating effect of trust on perceived privacy, this study also expects trust to have a moderating effect on perceived benefits. Studies integrating trust in the acceptance of technology have shown that trust has an effect on perceived usefulness, which is part of perceived benefits in this study (Belanche et al., 2012; Gefen et al., 2003). In another study is shown that perceived privacy risk, which is part of trust as described above, has a negative effect on perceived usefulness (Dong, Chang, Wang, & Yan, 2017). Following these results, this study expects trust to have a moderating effect on the relationship between perceived usefulness and acceptance of IoT applications. Accordingly, the following hypothesis has been made:

H4. Trust has a moderating effect on the relationship between privacy and benefits on acceptance, such that low trust will amplify the negative effect.

2.5 Conceptual model

Following the literature and the constructed hypotheses, the following conceptual model has been constructed.



3. Methodology

3.1 Participants

In this experiment, 122 participants (M_{age}= 32.28, SD_{age}=14.74, 60.7%female) participated by completing the survey. The participants voluntarily participated, but they were triggered to fill in the survey, since they had the chance to win a voucher with the value of 20, - euros from Bol.com. The respondents had to be eighteen years or older and living in the Netherlands. This study wanted to incorporate as much as possible different types of consumers, so it would be better generalizable to the rest of the Netherlands and result in a higher external validity. It was not necessary that the respondents had previously used IoT applications, considering the fact that the meaning of IoT applications has been explained in the beginning of the survey and this survey also wanted to incorporate potential new consumers for IoT applications. Respondents were recruited via social networks of the researcher. The survey was placed on the personal pages of the researcher on LinkedIn and Facebook. Besides, the survey was placed on closed group pages of Facebook, named 'Bedrijfs- en consumentenwetenschap jaar 2016/2017' (a group page for people who started their study Business- and consumer studies in 2016/2017) and 'Vragenlijst/Enquête RESPONDENTEN GEZOCHT/ruilen HBO/WO studenten' (a group page for students who are looking for respondents, within this group page you fill in each other's survey). Next to this, respondents were orally invited to fill in the survey and via direct messages on WhatsApp.

3.2 Design

Participants were randomly assigned to a 2 (Benefits: low vs. high) x 2 (Privacy revelation: low vs. high) between-subjects design. The four conditions in this study were: low privacy revelation and low benefits; high privacy revelation and low benefits; low privacy revelation and high benefits; high privacy revelation and high benefits.

3.3 Procedures and variables

The respondents firstly clicked on the link that was distributed via the network of the researcher, which directed them to the survey on Qualtrics. The respondents were welcomed and a general introduction was shown. Firstly, the subject of this research was told. Subsequently, anonymity and confidentiality was guaranteed to the respondents. The respondents had to agree to participate in this research under the stated conditions. When the respondents chose the option 'no, I don't want to participate in this research.', they were directed to the end of the survey. Otherwise they were send to the next page of the survey. In this page, an explanation of IoT applications was given. This explanation was necessary, since the IoT is a new upcoming industry and the researcher did not expect all of the respondents to understand the meaning of such new applications in advance. In this way every respondent had the same minimal amount of knowledge about IoT application, in order to participate in this research. After this explanatory section the respondents were asked the first questions in this survey, concerning trust in IoT applications.

The first questions were about the level of trust of the respondent in IoT applications in general. The respondents were asked to what extent they agreed with six statements (α=.805), adopted from Suh & Han (2002). Within these six statements the general trust of respondents in IoT applicants, the ability, the integrity and the benevolence of IoT applications were measured (e.g. 'IoT applications keep customers' best interest in mind'). They could indicate this on a 7-point Likert scale ranging from 'totally disagree' to 'totally agree'. These questions were related to the dependent variable 'trust', since it measures the level of trust in IoT applications.

Thereafter, Qualtrics assigned the respondents randomly to one of the four conditions. In the beginning of the conditions, a situation sketch was presented to the respondents. Using an example application, the Home Assistant, the respondents were told how many information they had to give up

in order to use this application. In the case of low or high privacy revelation, the respondents were told that the application does not or does monitor their lives continuously, respectively. Subsequently, the respondents were told what the benefits were of using this application. In the case of low or high benefits, the respondents were told that the application can only do something on their command or the application will perform activities on its own in the best interest of the respondent and gives suggestions for performing activities, respectively. In this way, the researcher influenced the independent variables 'perceived privacy' and 'perceived benefits'. The specific manipulation texts can be found in Appendix 1.

After the manipulation, all of the respondents, were directed to the remainder of the survey. The survey continued with the question about the acceptance of the application. Participants were asked to rate three statements (e.g. 'When I need such a Home assistant, I intent to use this one'; α=.948). regarding their acceptance on a 7-point Likert scale ranging from 'totally disagree' to 'totally agree'(Belanche et al., 2012). These statements were related to the dependent variable 'acceptance' ($M_{acceptance}$=4.765, $SD_{acceptance}$=1.571), because it measures consumers' intention to use the application. Thereafter, the respondents were asked a direct question about the acceptance of the Home assistant (e.g. 'Would you accept this Home assistant?'). They could answer this question with two option, 'yes' or 'no'. This question was asked to check whether the results were the same concerning the acceptance of the application, regardless the way it was asked, indirectly or directly.

In the next section, the consumers were asked two questions as a manipulation check: 'How much privacy-sensitive information should you reveal for the use of the application according to the situation sketch?' and 'How many benefits would you have with the use of the application according to the situation sketch?'

The respondents had two answer options to choose from, 'a lot of' or 'little/few'. These questions were asked to check whether the respondents had absorbed the manipulation while answering the questions about acceptance. Besides the manipulation check, the credibility of the situation sketch was also measured. The respondents were asked to what extent they agreed with the following statements: 'I have already used IoT applications before.' and 'I think that the situation sketch, about which I had to answer questions, could be a possible situation in reality.' They could indicate this on a 7-point Likert scale ranging from 'totally disagree' to 'totally agree'.

To conclude the questionnaire demographic questions about the respondent were asked, like gender and age. Thereafter, the respondents were debriefed, kindly thanked and able to leave some comments for the researcher. The full outline of the survey is added in Appendix 1.

4. **Results**

During the time the questionnaire was online, a small change has been made in the formulation of the manipulations text's. The first 30 participants read a different formulation than the subsequent participants. The meaning of the sentences remained the same, only the formulation differed a little. The effect of this change is expected to be very small, due to the fact that the meaning of the manipulation has not changed.

To check whether the participants absorbed the manipulations correctly, crosstabs have been made showing the percentages of their answers (low or high) to the questions of how many privacy sensitive information they had to reveal and how many benefits they got, according to the situation sketch (condition/manipulation) they had to read. For example, in the perfect situation, the percentages should be 100% for high privacy revelation and 100% for low benefits, when the participants where in the condition of High PR/ Low B.

Table 2: Manipulation Check. PR: Privacy revelation and B: Benefits

Manipulation Check				
	Privacy Revelation %		Benefits %	
Condition	High	Low	High	Low
Low PR/ Low B	18.8%	**81.3%**	37.5%	**62.5%**
Low PR/ High B	33.3%	**66.7%**	**70%**	30%
High PR/ Low B	**60%**	40%	33.3%	**66.7%**
High PR/ High B	**66.7%**	33.3%	**76.7%**	23.3%
% of Total	44.3%	55.7%	54.1%	45.9%

Binary logistic regressions have been conducted to check whether the predictor variables (conditions) 'amount of benefits' and 'amount of privacy revelation' predicted the outcome variables 'how many privacy sensitive information should you reveal, according to the situation sketch' and 'how many benefits would you get, according to the situation sketch' properly. To begin with the binary logistic regression for 'privacy revelation', the predictor 'privacy revelation' has an odds ratio of 4 (p=.011), which indicates that someone is 4 times more likely to decide that the amount of privacy revelation according to the situation sketch is high than low, when he or she is in the condition with a high amount of privacy revelation. For the manipulation check of 'privacy revelation', there was no effect of 'benefits' (p=.592) or the interaction (p=.545) between 'benefits' and 'privacy revelation'. Further, resulting from the binary logistic regression for 'benefits', the predictor 'benefits' has an odds ratio of 6.571 (p=.001), which indicates that someone is 6.571 times more likely to decide that the amount of benefits according to the situation sketch was high than low, when he or she is in the condition with high benefits. For the manipulation check of 'benefits', there was no effect of 'privacy revelation' (p=.560) or the interaction (p=.508) between 'benefits' and 'privacy revelation'. In general, it can be concluded that the manipulation has worked.

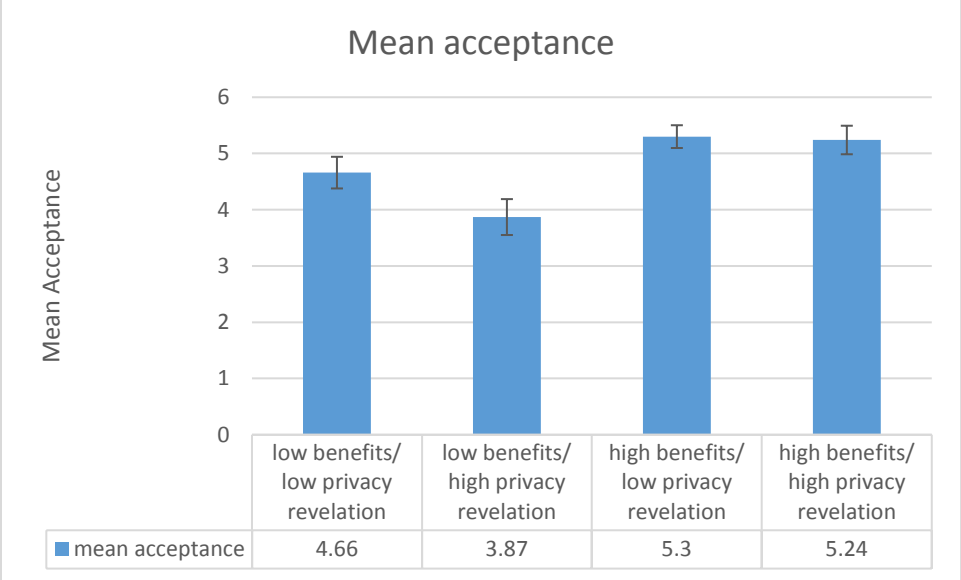
4.1 Benefits and Privacy Revelation

A two-way between-subjects ANOVA has been used to analyse hypothesis 1 (The Perceived Benefits will have a positive effect on the acceptance of IoT applications) and hypothesis 2 (The amount of revelation of personal information, will have a negative effect on the acceptance of IoT applications). The dependent variable was the composed mean of acceptance, which is a scale variable. The independent nominal variables were the amount of benefits and the amount of privacy revelation, which could be either high or low.

There was a statistically significant main effect of Perceived Benefits on the acceptance of IoT applications ($F(1,122)=14.20$, $p<0.001$). Participants in the low level of benefits condition ($M=4.26$, $SD=0.19$) have a significantly lower level of acceptance than participants in the high level of benefits condition ($M=5.27$, $SD=0.19$), regardless of the level of privacy revelation (see Figure 1). Therefore, hypothesis 1, stating that perceived benefits will have a positive effect on the acceptance of IoT, can be accepted.

In contrast, there was not a statistically significant main effect for the amount of privacy revelation on the acceptance of IoT applications ($F(1,122)=2.48$, $p=.118$). Figure 1 shows a difference in the levels of acceptance between the conditions of low amount of privacy revelation and high amount of privacy revelation. The conditions of low privacy revelation have a higher level of acceptance compared to the conditions of high privacy revelation, regardless of the level of benefits. Nevertheless, this difference was not big enough to be statistically significant. Therefore, hypothesis 2, stating that the amount of revelation of personal information will have a negative effect on the acceptance of internet of things, will be rejected.

Figure 1: mean acceptance in the 4 conditions



Despite the fact that hypothesis 2 has been rejected, it is worthwhile noticing that the data shows some interesting things. In the case of high benefits, the difference in acceptance is little between the two conditions of privacy revelation, and in the case of low benefits the difference in acceptance is relatively big between the two conditions of privacy revelation.

To analyse hypothesis 3a (If the benefits are high, the acceptance will be positively affected, regardless of the level of the privacy revelation), hypothesis 3b (A combination of low benefits and low privacy revelation will have a positive effect on the acceptance) and hypothesis 3c (A combination of low benefits and high privacy revelation will have a negative effect on the acceptance) the same two-way ANOVA has been used as above.

There was not a statistically significant interaction effect between the amount of benefits and the amount of privacy revelation, ($F(1,122)=1.87$, $p=.174$). Despite the fact that there was not a significant interaction effect, some interest things could be seen in the data.
In the conditions with high benefits (High benefits/ low privacy revelation: $M=5.30$, $SD=0.27$; High benefits/ high privacy revelation: $M=5.24$, $SD=0.27$) the acceptance was higher compared to the conditions with low benefits ($M=4.66$, $SD=0.26$; $M=3.87$, $SD=0.27$), regardless of the level of privacy revelation. However, the interaction effect is not significant and hypothesis 3a will be rejected.

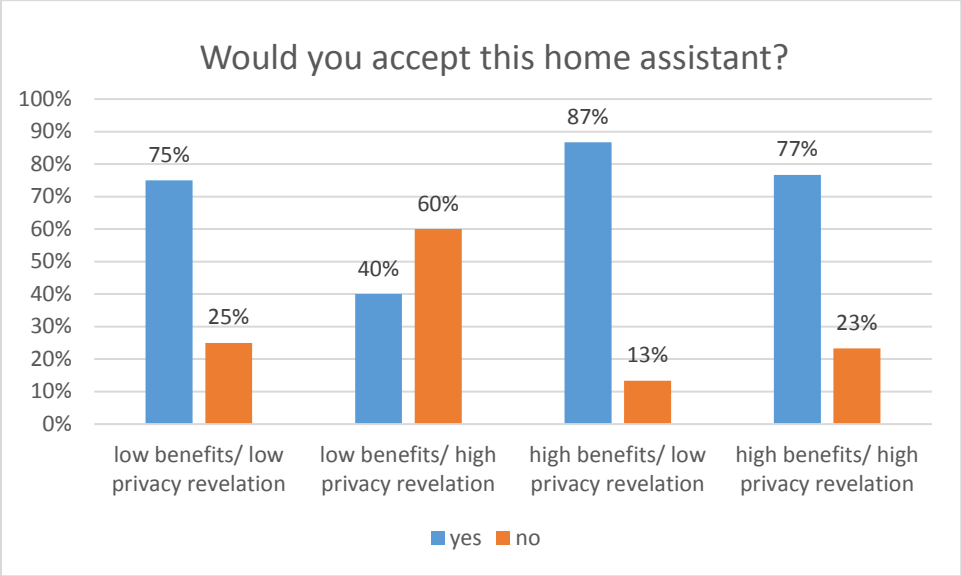
Subsequently, the data showed a difference in means of 0.789 between the conditions 'low benefits/ high privacy revelation' ($M=3.87$, $SD=0.27$) and 'low benefits/ low privacy revelation' ($M=4.66$, $SD=0.26$). The question measuring acceptance were answered on a 7-point Likert scale, with 4 as the mean. Despite the fact that the mean of 'low benefits/ low privacy revelation' was above 4, hypothesis 3b will be rejected, because there is not a significant interaction effect.

Next to this, hypothesis 3c will also be rejected, because of the insignificant interaction effect.

In order to check the result from the two-way ANOVA, a secondary direct question was asked to the participants (i.e. 'Would you accept this Home Assistant?'). A binary logistic regression has been conducted and a Bar Chart has been made of this question. The binary logistic regression showed that someone, who is in the condition of high benefits, is 4.93 times more likely to answer with 'yes' instead of 'no' ($P=.005$). The outcomes of privacy revelation (odds ratio= 0.505, $p=.322$) and the interaction between benefits and privacy revelation (odds ratio=0.44, $p=.352$) were again not significant. This corresponds with the outcomes of the two-way ANOVA.

Figure 2 shows the percentages of acceptance following the question 'Would you accept this home assistant?' in the four different conditions. In almost all off the conditions the percentages of 'yes' are higher than the percentages of 'no', except for the condition of 'Low benefits/ high privacy revelation'. These results would support hypothesis 3a, 3b and 3c, however there is no statistical evidence.

Figure 2: percentages yes and no for the question 'Would you accept this home assistant?'



4.2 Trust in IoT applications

To research the direct effect of trust on the acceptance of IoT applications, hypothesis 5 (Trust has a positive effect on the acceptance of IoT applications) was constructed.

A simple linear regression was calculated to predict acceptance based on trust. Table 3 shows that there was a significant result. The slope coefficient for acceptance was 0.526 and the constant was 2.408. So, with an increase of 1 in trust, acceptance increased with 0.526. Based on this, hypothesis 5 can be accepted.

Table 3: Coefficients of simple linear regression to predict acceptance based on trust

Coefficients								
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95,0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	2.408	.682		3.530	.001	1.057	3.758
	Mean Trust	.526	.149	.307	3.528	.001	.231	.821

4.3 Moderating effect of Trust

To test if there is a moderating effect of trust on the interaction between privacy revelation and benefits, hypothesis 4 (Trust has a moderating effect on the relationship between privacy and benefits on acceptance, such that low trust will amplify the negative effect) was constructed.

In order to analyse the effect of the covariate trust in the interaction between benefits and privacy revelation and its effect on acceptance, an ANCOVA has been conducted with the composed mean of trust as covariate. The dependent variable was still the composed mean of acceptance and the other independent variables were still the amount of benefits and the amount of privacy revelation.

Table 4: ANCOVA results with Trust as covariate

Dependent Variable: Mean Acceptance		
Source	F	Sig.
Corrected Model	4.599	0
Intercept	20.95	0
Benefits	2.189	0.142
PrivacyRevelation	2.801	0.097
Mean_Trust	5.432	0.022
Benefits * PrivacyRevelation	1.631	0.204
Benefits * Mean_Trust	0.762	0.385
PrivacyRevelation * Mean_Trust	1.928	0.168
Benefits * PrivacyRevelation * Mean_Trust	2.071	0.153

There was a statistically significant effect of trust. The covariate trust significantly predicts the values of the dependent variable acceptance ($F(1,122)=5.43$, $p=.022$). With the use of ANCOVA, the

interaction between Benefits*PrivacyRevelation*MeanTust, has also been analysed in order to see if hypothesis 4 can be accepted. Following these results, trust has not a moderating effect on the relationship between privacy revelation and benefits, such that low trust will amplify the negative effect ($F(1,122)=2.071$, $p=.153$). Therefore, hypothesis 4 will be rejected.

Table 5: hypothesis results

Hypothesis	Accepted/rejected
H1. The Perceived Benefits will have a positive effect on the acceptance of IoT applications.	**accepted**
H2. The amount of revelation of personal information, will have a negative effect on the acceptance of IoT applications.	**rejected**
H3a. If the benefits are high, the acceptance will be positively affected, regardless of the level of the privacy revelation.	**rejected**
H3b. A combination of low benefits and low privacy revelation will have a positive effect on the acceptance.	**rejected**
H3c. A combination of low benefits and high privacy revelation will have a negative effect on the acceptance.	**rejected**
H4. Trust has a moderating effect on the relationship between privacy and benefits on acceptance, such that low trust will amplify the negative effect.	**rejected**
H5. Trust has a positive effect on the acceptance of IoT applications.	**accepted**

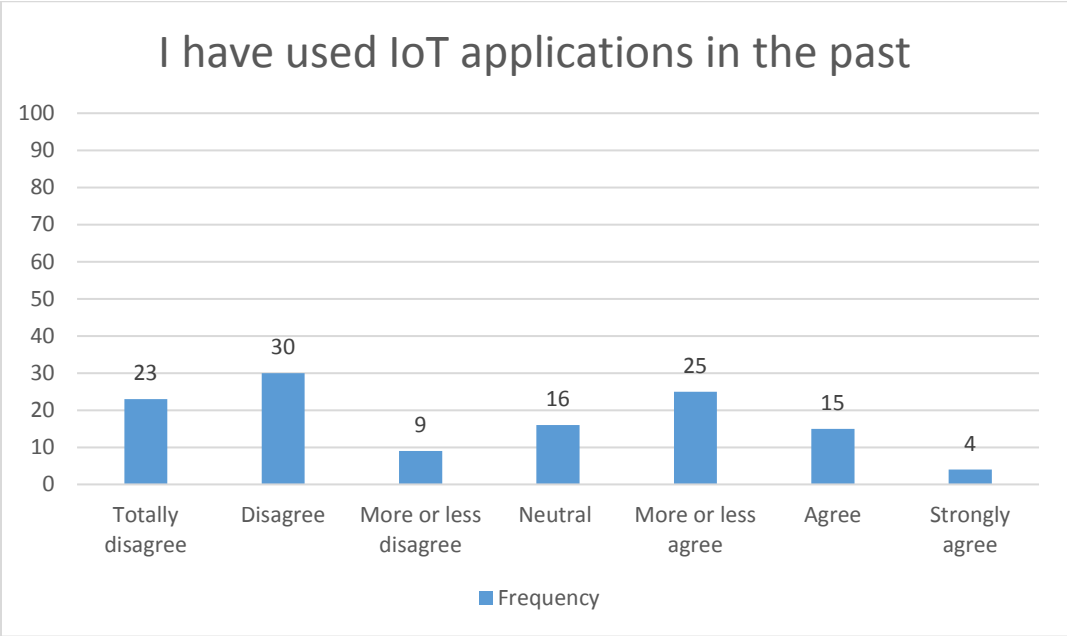
4.4 Additional Analyses

Next to the hypothesis which has been made in advance, an additional analysis has been done on the relationship between age and acceptance. It may be the fact that there is a relationship between age and acceptance, since elderly people may be less familiar with technology than younger people. However, the data did not show this relationship. A simple linear regression has been conducted to predict acceptance based on age. Age did not significantly predict acceptance ($\beta=0.004$, $t(120)=0.43$, $p=.607$), with a R^2 of .002.

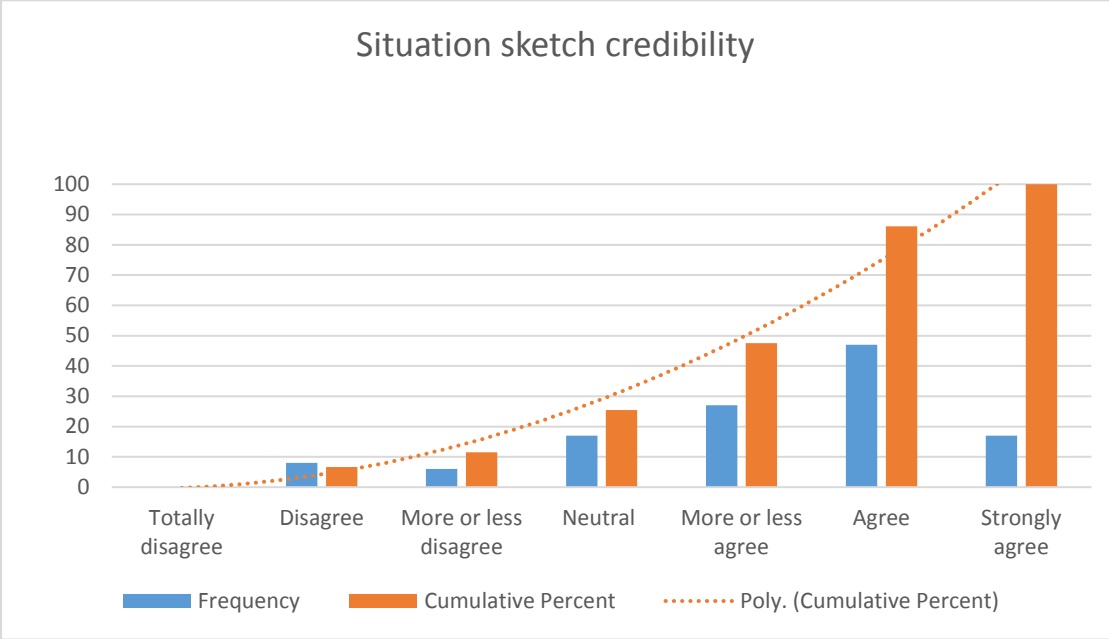
Besides, a graphic has been made of the questions 'I have used IoT applications in the past' (see Graph 1, next page). This table showed that 62 participants had not used IoT application (a lot) before, and the other 60 participants had used IoT applications (a lot) before. Subsequently, a simple linear regression has been conducted to predict acceptance with the question 'I have used IoT applications in the past'. The question 'I have used IoT applications in the past' significantly predicted acceptance ($\beta=0.205$, $t(120)=2.73$, $p=.007$), with a R^2 of .06. With an increase of 1 in IoT experience, acceptance increased with 0.205.

Further, a graphic has been made of the question 'The situation sketch, about which I had to answer some questions, could be a possible situation in real-life' (see Graph 2, next page). This table showed that 81,9% of the participants answered neutral…totally agree, so most of the participants thought that the situation sketch could be a possible situation in real-life.

Graph 1: Frequencies of the statement 'I have used IoT applications in the past'



Graph 2: Frequencies and cumulative percent of the statement 'The situation sketch, about which I had to answer some questions, could be a possible situation in real-life'



5. Discussion

The market of the IoT is rapidly growing and more and more consumers are starting to use IoT application. Although, it is a new market, with relatively little research being done within this market. Currently, a lot of research has been done on the acceptance of technology in general. Several theories have been created to analyse the acceptance of technology, however little consumer research has been done with respect to the acceptance of IoT application. With the use of IoT applications, consumers must be willing to give up parts of their privacy, in order to let the applications do their work. In return, the consumers receive benefits with the use of IoT applications. So, there is a trade-off between perceived privacy and perceived benefits. Earlier research has shown that consumers intend to compare the ratio of outputs (benefits) and the ratio of inputs (cost) (J. S. Adams, 1963). Subsequently, consumers intending to use a IoT application may weigh the perceived benefits against the perceived privacy and chose whether they would use the application. At the moment, little research has been done to the trade-off between perceived benefits and perceived privacy and its effect on the acceptance of IoT applications. Therefore, this study researched this trade-off in order to see what the effect of this trade-off is on the acceptance of IoT applications.

Making IoT applications more beneficial, did influence the acceptance of IoT applications. The results showed that the amount of perceived benefits influenced the acceptance of IoT applications in a positive way. This can be explained by the theories TAM (Davis et al., 1989) and UTAUT (Venkatesh et al., 2003). In these two theories, perceived ease of use and perceived usefulness are being used to predict the acceptance of technology. Following these two theories, the acceptance would increase when these 2 factors are positively influenced. The current study showed the same results, when the perceived benefits (perceived usefulness and perceived ease of use) increased, the acceptance of the IoT application also increased. In this way, marketers of IoT applications can make the applications more acceptable by pointing out the ease of use and the developers can make the applications more acceptable by enhancing the usefulness.

Surprisingly, did the amount of perceived privacy not have a significant effect on the acceptance of the IoT application. However, the data showed some differences regarding to the effect of perceived privacy on the acceptance of IoT applications, in different conditions. The effect of perceived privacy differed between the conditions of low benefits and high benefits. When the benefits were high, the amount of perceived privacy did not affect the acceptance of IoT applicant a lot. There was just a small difference in the means of acceptance between the conditions ‘high benefits/ low privacy revelation’ and ‘high benefits/ high privacy revelation’. In contradiction, the data showed a larger difference in means between the conditions ‘low benefits/ low privacy revelation’ and ‘low benefits/ high privacy revelation’. When the benefits are low, the amount of privacy revelation seems to have a negative effect on the acceptance of IoT application, however there is not any statistical evidence for this. An explanation for the different effects of perceived privacy, between low perceived benefits and high perceived benefits, may be that it does not matter how much information consumers need to reveal as long as the benefits are high. When the benefits are low, consumers may not be willing to reveal (a lot of) information, since there is no gain in the trade-off for them. These insights are interesting for the IoT industry. Marketers and developers should keep in mind that there are differences in the levels of acceptance between the two conditions with low benefits. For example, if the marketers and developers introduce a new IoT application which has lower benefits than competitor applications, but will gain more features/benefits in the future. They should not ask for the same high level of privacy revelation as competitor applications, since their application is in the condition of low benefits. When the benefits are high, marketers and developers can be more free in the amount of personal information consumers need to reveal. In general, it seems to be the case that the acceptance of IoT applications is positively being influenced by a higher level of perceived benefits. For the effect of perceived privacy is no statistical evidence, but it is worthwhile mentioning that the data showed difference in the acceptance between ‘low benefits/ low privacy revelation’ and ‘low benefits/ high privacy revelation’. Thus, as long as the amount of benefits are high, consumers are willing to give up their privacy.

Next to the trade-off between privacy revelation and the amount of benefits and its effect on acceptance, the effect of trust has also been researched. This study showed that there is a positive relationship between the level of trust in IoT applications and the level of acceptance. A significant higher level of acceptance can be observed when trust rises among the consumers. Besides the direct relationship between trust and acceptance, trust has not a moderating effect on the interaction between benefits and privacy and its effect on acceptance. In the case of a negative effect of the relationship between benefits and privacy on acceptance, it has not been proven that low trust will amplify this negative effect. Overall, there is a positive relationship between trust in IoT technology and the acceptance of IoT applications. The fact that trust has an important influence on the acceptance of IoT applications, is also supported by earlier research. According to Yildirim and Ali-Eldin (2018), is trust a significant factor that influences the intention to use IoT applications. This is an important finding for the developers of IoT applications, since they can make sure that the applications are trustworthy. AlHogail (2018) mentioned that developers of IoT applications need to make sure that the applications act as expected, in order to guarantee consumer trust, even in a hostile environment.

Finally, the relationship between age and the acceptance has been analysed. The analysis showed that there was not a significant relationship between age and acceptance. It could had been the case that the acceptance of IoT applications decreases as the age rises. The reasoning behind this is that younger consumers may be are more often using technology and may be more used to these new technologies. Elderly consumers may be afraid of new technologies and less willing to accept it, since they may be less familiar with it. Nevertheless, this has not been found in this study.

5.1 Theoretical and practical relevance

The theoretical relevance of this study is, that it researches the effect of the amount of privacy revelation in combination with the amount of benefits on the acceptance of IoT applications. No study has done this before. The amount om privacy revelation is a new parameter that has been used in research to the acceptance of IoT applications. It makes this study unique that it incorporates the equity theory/ privacy calculus and the TAM/ UTAUT in one study. Within these separate theories, researchers studied trade-offs between benefits and costs in general (equity/ privacy calculus) and models to analyse the acceptance of technology in general. Different aspect of these theories has been used in the experiment of this study. In this way a new theoretical construct has been created, which can be used to analyse to which extend consumers are willing to give up their privacy in order to use IoT applications. So, on the basis of general acceptance models for IoT applications and general trade-off models, this study is the first to implement a new unique construct that measures the effect of different levels of privacy revelation and different level of benefits on the acceptance. Besides, this study confirms the finding of earlier research, that trust has a direct effect on the acceptance of IoT (AlHogail, 2018; Belanche et al., 2012; Gao & Bai, 2014; Khan et al., 2016; Yildirim & Ali-Eldin, 2018).

Next to the theoretical relevance, this study has also practical relevance. As stated in the beginning of this thesis, is the market of IoT rapidly growing. More and more IoT applications are entering the market and the IoT are being applied in a wide range of contexts. There is a challenge for marketers and developers to create applications for consumers, which are as attractive as possible. Results from this study can support those marketers and developers during the creation of new applications in order to enhance the acceptance of the applications. Firstly, this study generates insights, for marketers and developers, in the extent to which consumers are willing to give up their privacy. With these insights, they can adjust their IoT applications and respond better to the requirements of the consumer. Secondly, this study emphasizes the importance of trust in IoT applications for the acceptance of IoT applications. There is a task for the marketers and developers to create a certain level of trust by the consumer and make sure the applications work as promised. Companies can take their advantage with these insights and make IoT applications more accepted by consumers.

5.2 Limitations and future research

The first limitation of this study was the age distribution of the participants. The ages were concentrated around 20-21 years old. With this concentrated distribution, the outcomes of the study cannot be generalized to a wide range of ages in the Netherlands. Therefore, in future research, the distribution of ages should be better controlled by the researcher. Additionally, this study had only 122 participants, despite the fact of using all of the social networks of the researcher. More participants should be used in future research, in order to make the study more generalizable.

Next to this, this study focussed on one particular application. By studying the effect of different conditions on the acceptance of this particular application, this study tried to generate some general insights in the field of IoT applications. It was not possible to incorporate all of the IoT applications nor one application in every context (e.g. smart cities, smart building, smart health) in one study. The results could have differed in different context. For example, in the context of smart health the willingness to reveal privacy sensitive information may differ from the context of smart cities. Nevertheless, the Home Assistant was the most suitable application to use in this study, because the benefits and the amount of privacy revelation had to be manipulated, while the application should be able to work in all of the conditions. Besides, the home assistant was the most suitable application, since it is part of the context of smart homes. Within the environment of smart homes personal information is intensively being monitored. In addition, a reason to choose smart home appliances, is the applicability of these appliances for almost all of the consumers. As described in the literature chapter, not everyone suffers from health problems and not everyone is able to drive a vehicle, but almost everyone is living in a home. Future research should be conducted, to specifically analyse the effect on different applications and in different IoT contexts.

Furthermore, a suggestion with respect to the conditions could be made. Within this study, 4 conditions were created. Within these conditions, only extreme values were presented. For example, the participant was in the condition of high or low benefits, there were no intermediate values possible. In order to research the effects of the amount of benefits and the amount of privacy revelation on the acceptance more sophisticated, more conditions could be created in which average amounts of benefits and privacy revelation are given. In this way, the researcher will be better able to see the effects along the line of benefits and privacy and see whether there is a threshold in acceptance.

Finally, research could be done to the acceptance of IoT applications, with the same conceptual model, but instead of manipulating the participants with situation sketches, the researcher could give the participants a manipulated Home Assistant in real-life. Subsequently, the researcher can measure whether the participants would accept it when they have to give up information in real-life and receive the benefits in real-life. By doing this one can check whether there are differences in the effects of perceived privacy and perceived benefits on the acceptance of IoT application between real-life situations and hypothetical (situation sketch) situations.

6. Conclusion

Altogether, the market of the IoT is booming at the moment. Lots of new applications are being developed and the market of IoT in itself is already new for consumers. That is why it is important, among other things, to reflect on the trade-off between perceived privacy revelation and perceived benefits of these new IoT applications, in order to enhance the acceptance. Researching the effects of privacy revelation is a whole new idea. It is important to know, to what extend perceived privacy and perceived benefits have an effect on the acceptance of IoT applications, for companies selling these applications. This study found that perceived benefits have a positive effect on the acceptance. However, this study did not found an effect for perceived privacy revelation on the acceptance. Next to this, is trust in a product and/or company also important for the acceptance of products. This is supported by the findings of this study, there was a positive relationship between the level of trust and the level of acceptance of IoT applications. So, trust directly influence the acceptance, however trust has not a moderating effect on the relationship between perceived benefits and perceived privacy revelation on acceptance. Adding benefits to the applications and building trust are the most important things with respect to the acceptance of IoT applications.
In other words, keep up the high benefits and level of trust or die trying.

References

Abaker Targio HAshem, I., Chang, V., Anuar, N. B., Adewole, K., Yaqoob, I., Ahmed, E., & Chiroma, H. (2016). The role of big data in smart city. *International Journal of Information Management*, *36*(5), 748. https://doi.org/http://dx.doi.org.ezproxy.library.wur.nl/10.1016/j.ijinfomgt.2016.05.002

Adams, J. S. (1963). TOWARD AN UNDERSTANDING OF INEQUITY. *Journal of Abnormal and Social Psychology*, *67*(5), 422–436. https://doi.org/10.1037/h0040968

Adams, M. (2017). Big Data and Individual Privacy in the Age of the Internet of Things, *7*(4), 12. Retrieved from www.timreview.ca

Al-Momani, A. M., Mahmoud, M. A., & Ahmad, M. S. (2016). Modeling the adoption of internet of things services: A conceptual framework. *International Journal of Applied Research*, *2*(5), 361–367.

AlHogail, A. (2018). Improving IoT Technology Adoption through Improving Consumer Trust. *Technologies*, *6*(3), 64. https://doi.org/10.3390/technologies6030064

Apthorpe, N., Reisman, D., Sundaresan, S., Narayanan, A., & Feamster, N. (2017). Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic. https://doi.org/10.1109/TNSM.2009.090604

Belanche, D., Casaló, L. V., & Flavián, C. (2012). Integrating trust and personal values into the technology acceptance model: The case of e-government services adoption. *Cuadernos de Economia y Direccion de La Empresa*, *15*(4), 192–204. https://doi.org/10.1016/j.cede.2012.04.004

Culnan, M. J., & Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science*, *10*(1), 104–115. https://doi.org/10.1287/orsc.10.1.104

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, *35*(8), 982–1003. https://doi.org/10.1287/mnsc.35.8.982

Dlodlo, N., Foko, T., Mvelase, P., & Mathaba, S. (2012). The State of Affairs in Internet of Things Research. *The Electronic Journal of Information Systems Evaluation*, *15*(3), 244–258. https://doi.org/10.1016/j.apmr.2005.07.291

Dong, X., Chang, Y., Wang, Y., & Yan, J. (2017). Understanding usage of Internet of Things (IOT) systems in China: Cognitive experience and affect experience as moderator. *Information Technology and People*, *30*(1), 117–138. https://doi.org/10.1108/ITP-11-2015-0272

Fishbein, M., & Ajzen, I. (1975). *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research*. Reading, Massachusetts: Addison-wesley.

Gao, L., & Bai, X. (2014). A unified perspective on the factors influencing consumer acceptance of internet of things technology. *Asia Pacific Journal of Marketing and Logistics*, *26*(2), 211–231. https://doi.org/10.1108/APJML-06-2013-0061

Gefen, D., Karahanna, E., & Straub, detmar w. (2003). Trust and TAM in online shopping : An integrated model. *MIS Quarterly*, *27*(1), 51–90.

Grandison, T., & Sloman, M. (2000). A survey of trust in internet applications. *IEEE Communications Surveys & Tutorials*, *3*(4), 2–16. https://doi.org/10.1109/COMST.2000.5340804

Guerrero, L. K., A. Andersen, P., & Afifi, W. (2014). *Close Encounters: Communication in Relationships* (4th editio). Los Angeles: CA: Sage Publications Inc.

Hann, I.-H., Hui, K.-L., Tom Lee, S.-Y., & Ivan, P. L. P. (2007). Overcoming online information privacy concerns: an information-processing theory approach. *Journal of Management Information Systems*, *24*(2), 13–42.

Hornby, A. S., Cowie, A. P., & Gimson, A. C. (1988). *Oxford Advanced Learner's Dictionary of Current English*. Oxford: Oxford University Press.

Khan, W., Aalsalem, M., Quratulain, A., & Khan, M. (2016). Enabling Consumer Trust Upon Acceptance of IoT Technologies Through Security and Privacy Model. *Advanced Multimedia and Ubiquitous Engineering*, *354*, 479–485.

Ku, Y., Li, P., & Lee, Y. (2018). *Are You Worried About Personalized Service? An Empirical Study of the Personalization-Privacy Paradox* (Vol. 10923). Springer International Publishing. https://doi.org/10.1007/978-3-319-91716-0_27

Lee, S., Ha, H. R., Oh, J. H., & Park, N. (2018). *The Impact of Perceived Privacy Benefit and Risk on Consumers' Desire to Use Internet of Things Technology* (Vol. 10905). Springer Verlag. https://doi.org/10.1007/978-3-319-92046-7_50

Leong, G. W., Ping, T. A., & Muthuveloo, R. (2017). Antecedents of Behavioural Intention to Adopt Internet of Things in the Context of Smart City in Malaysia. *Global Business and Management Research: An International Journal*, *9*(4s), 442–456.

Majumdar, A., & Bose, I. (2016). Privacy Calculus Theory and Its Applicability for Emerging Technologies (pp. 191–195). Springer International Publishing. https://doi.org/10.1007/978-3-319-45408-5_20

Milne, G. R., Pettinico, G., Hajjat, F. M., & Markos, E. (2017). Information Sensitivity Typology: Mapping the Degree and Type of Risk Consumers Perceive in Personal Data Sharing. *Journal of Consumer Affairs*, *51*(1), 133–161. https://doi.org/10.1111/joca.12111

Patel, K., & Patel, S. (2016). Internet of Things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges. *International Journal of Engineering Science and Computing*, *6*(5), 6122–6131. https://doi.org/10.4010/2016.1482

Poushneh, A. (2018). Augmented reality in retail: A trade-off between user's control of access to personal information and augmentation quality. *Journal of Retailing and Consumer Services*, *41*(January), 169–176. https://doi.org/10.1016/j.jretconser.2017.12.010

Pretz, K. (2013). The Next Evolution of the Internet. Retrieved November 5, 2018, from http://theinstitute.ieee.org/technology-topics/smart-technology/the-next-evolution-of-the-internet

Suh, B., & Han, I. (2002). Effect of trust on customer acceptance of Internet banking. *Electronic Commerce Research and Applications*, *1*(3–4), 247–263. https://doi.org/10.1016/S1567-4223(02)00017-0

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). USER ACCEPTANCE OF INFORMATION TECHNOLOGY: TOWARD A UNIFIED VIEW, *27*(3), 425–478. https://doi.org/10.2307/30036540

Vermesan, O., & Friess, P. (2013). *Internet of Things : Converging Technologies for Smart Environments and Integrated Ecosystems*. (O. Vermesan & P. Friess, Eds.). Aalborg: River Publishers Series in Communication. Retrieved from http://www.internet-of-things-research.eu/pdf/Converging_Technologies_for_Smart_Environments_and_Integrated_Ecosystems_IERC_Book_Open_Access_2013.pdf

Weinberg, B. D., Milne, G. R., Andonova, Y. G., & Hajjat, F. M. (2015). Internet of Things: Convenience vs. privacy and secrecy. *Business Horizons*, *58*(6), 615–624. https://doi.org/10.1016/j.bushor.2015.06.005

Wilson, D., & Valacich, J. (2012). Unpacking the Privacy Paradox: Irrational Decision-Making within the Privacy Calculus. *Proceedings of the 33rd International Conference on Information Systems*, 1–11.

Xiu, D., & Liu, Z. (2005). A Formal Definition for Trust in Distributed Systems. *Information Security Conference 2005*, 482–489. https://doi.org/10.1007/11556992_35

Yildirim, H., & Ali-Eldin, A. M. T. (2018). A model for predicting user intention to use wearable IoT devices at the workplace. *Journal of King Saud University - Computer and Information Sciences*, 1–9. https://doi.org/10.1016/j.jksuci.2018.03.001

Appendix 1: survey outline

Bedankt dat u mee wilt doen aan dit onderzoek. Ik ben een Bachelor student Bedrijfs- en Consumentenwetenschappen en doe onderzoek naar de acceptatie van Internet of Things (in de vragenlijst aangeduid met de afkorting 'IoT') applicaties. Ik zal in de volgende pagina's een uitleg geven over IoT applicatie zodat u weet waarover u vragen beantwoord.

Het invullen van deze vragenlijst is geheel vrijwillig. Het invullen van de vragenlijst zal ongeveer 5 minuten duren. Vult u alstublieft in wat het eerste bij u op komt. Er zijn in deze vragenlijst geen goede of foute antwoorden, ik ben slechts geïnteresseerd in uw gedachtegang. Door deel te nemen aan deze vragenlijst maakt u kans om een waardebon van €20,- voor bol.com te winnen. Uw antwoorden zullen anoniem blijven en er zal met respect en vertrouwen mee worden omgegaan. De antwoorden zullen enkel gebruikt worden voor dit onderzoek.
Door op 'ja' te klikken geeft u aan het bovenstaande gelezen te hebben en hier mee akkoord te gaan.

- Ja, ik neem deel aan het onderzoek.
- Nee, ik wil niet deelnemen aan het onderzoek.

Uitleg Internet of Things (IoT) applicaties:
The Internet of Things, oftewel het Internet der Dingen, is een netwerk van slimme objecten die met elkaar verbonden zijn via het internet. Bij deze objecten kunt u aan van alles denken, van uw koffiezet apparaat die automatisch aangeeft wanneer een onderdeel vervangen moet worden tot lantarenpalen die automatisch aan gaan wanneer u komt aanrijden. Deze IoT applicatie kunnen op allerlei gebieden worden ingezet om u, andere personen en producten te monitoren en op basis van die gegevens u te ondersteunen. Denk aan de gebieden: slimme steden (suggesties voor parkeerplekken o.b.v. uw locatie); slimme huizen (koelkast die aangeeft wanneer iets over de datum gaat); slimme zorg (object die uw hartslag meet en kan ingrijpen wanneer u een hartaanval krijgt). In ruil daarvoor zal u bereid moeten zijn dat deze IoT applicatie, u, andere personen en objecten mag monitoren.

1. In hoeverre bent u het eens met de volgende stellingen?
Op een schaal van (1) 'helemaal mee oneens' tot (7) 'helemaal mee eens'

- IoT applicaties zijn betrouwbaar.
- Ik vertrouw op de voordelen van de beslissingen van IoT applicaties.
- IoT applicaties houden zich aan hun beloften en verplichtingen.
- IoT applicaties houden het belang van de klant in het achterhoofd.
- IoT applicaties zouden het werk goed doen, zelfs als ze niet worden bewaakt.
- Ik vertrouw IoT applicaties.

Manipulaties

- Conditie 1 (Low privacy revelation, low benefits)
  Stel je voor

  Je hebt in de toekomst een ver doorontwikkelde IoT applicatie gekocht, genaamd de Home assistent.
  Voor het gebruik van de Home assistent hoef je **weinig informatie vrij te geven**. Hij voert alleen acties uit op jouw commando en monitort niet jouw leven. Je hebt **weinig voordelen** aan de Home assistent. Hij kan bijvoorbeeld alleen de verwarming aanzetten of boodschappen bestellen wanneer jij dat aangeeft.

- Conditie 2 (Low privacy revelation, high benefits)
  Stel je voor

  Je hebt in de toekomst een ver doorontwikkelde IoT applicatie gekocht, genaamd de Home assistent.
  Voor het gebruik van de Home assistent hoef je **weinig informatie vrij te geven**.
  Hij voert actie uit op jouw commando en monitort niet jouw leven.
  Je hebt **veel voordelen** aan de Home assistent. Hij doet de volgende dingen als jij erom vraagt: Boodschappen bestellen, verwarming aanzetten, muziek afspelen.
  Hij kan ook suggesties geven voor het uitvoeren van activiteiten.

- Conditie 3 (high privacy revelation, low benefits)
  Stel je voor

  Je hebt in de toekomst een ver doorontwikkelde IoT applicatie gekocht, genaamd de Home assistent.
  Voor het gebruik van de Home assistent moet je **veel informatie vrijgeven**. Hij houdt continu jouw agenda bij en volgt jouw activiteiten, hij luistert continu mee in de woonkamer, hij houdt bij wat je eetpatroon is en wat je temperatuur voorkeur is.
  Je hebt **weinig voordelen** aan de Home assistent, aangezien hij alleen activiteiten uitvoert als jij erom vraagt. Hij kan bijvoorbeeld de verwarming aanzetten of boodschappen bestellen als jij dat wilt.

- Conditie 4 (high privacy revelation, high benefits)
  Stel je voor

  Je hebt in de toekomst een ver doorontwikkelde IoT applicatie gekocht, genaamd de Home assistent.
  Voor het gebruik van de Home assistent moet je **veel informatie vrijgeven**. Hij houdt continu jouw agenda bij en volgt jouw activiteiten, hij luistert continu mee in de woonkamer, hij houdt bij wat je eetpatroon is en je temperatuur voorkeuren.
  Je hebt **veel voordelen** aan de Home assistent. Hij zet de verwarming aan als je naar huis rijdt; Hij besteld boodschappen als producten dreigen op te raken in de koelkast; Hij volgt commando's op (bijv. 'Speel de top 40 van Spotify af'); Hij herinnert je aan afspraken die in je agenda staan.

Zelfde set vragen voor alle condities
2. In hoeverre bent u het eens met de volgende stellingen?
Op een schaal van (1) 'helemaal mee oneens' tot (7) 'helemaal mee eens'
Wanneer ik zo'n Home assistent nodig heb …
- …heb ik de intentie om deze te gebruiken.
- …voorspel ik dat ik deze zal gebruiken.
- …zou ik graag deze willen gebruiken.

3. Zou u deze Home assistent accepteren?
Ja/nee

4. Hoeveel privacygevoelige informatie zou u voor het gebruik van de beschreven Home assistent moeten opgeven?
Veel/weinig

5. Hoeveel voordelen zou u hebben aan het gebruik van de beschreven Home assistent?
Veel/weinig

6. In hoeverre bent u het eens met de volgende stellingen?
Op een schaal van (1) 'helemaal mee oneens' tot (7) 'helemaal mee eens'

- Ik heb in het verleden al vaker IoT applicaties gebruikt.
- Ik denk dat de geschetste situatie, waarover ik vragen moest beantwoorden, een mogelijk situatie kan zijn in de werkelijkheid.

7. Ik ben een …
Man/vrouw

8. Wat is uw leeftijd? (Dropdown list)

9. Wanneer u kans wilt maken op een bol.com bon vul dan hier uw email adres in: …

Ik wil u hartelijk bedanken voor het invullen van deze vragenlijst. Het doel van dit onderzoek is om te kijken in hoeverre men bereid is om informatie op te geven voor de voordelen van IoT applicaties en het effect hiervan op de acceptatie van deze applicaties. Ik zal 4 januari via het opgegeven email adres bekend maken of u de gelukkig winnaar bent geworden voor de bol.com waardebon. Als u nog opmerkingen of toelichten heeft kunt u deze hieronder invullen.

Indien u verdere vragen of opmerkingen heeft, kunt u contact opnemen met Karsten van 't Wel via het volgende email adres: karsten.vantwel@wur.nl.

Heel erg bedankt voor uw moeite en tijd!