The Relationship between Transparency, Consumer Trust and Willingness to Share Data – A Vignette Survey

Author: Jana Marina Rickert
University of Twente
P.O. Box 217, 7500AE Enschede
The Netherlands

ABSTRACT **A new era of technology and connected living is introduced by the Internet of Things industry. Although it is one of the most promising domains of the future, security issues and privacy concerns have kept it from revolutionizing business sectors of any kind. Since collecting and analyzing data is what the Internet of Things is based on, knowing what makes people share sensitive information is crucial to every company wanting to establish itself in this new industry. Therefore, the goal of this study is to identify factors positively influencing people's willingness to share their data. Derived from driving factors of willingness to share data online, consumer trust and transparency of data were investigated as influencing factors on sharing data for Internet of Things devices. To explore the relationship between consumer trust, transparency of data and willingness to share, empirical research was conducted. A vignette survey was used to avoid bias and ensure respondents apply their answers to an Internet of Things device. Four scenarios were presented to the respondent, to which he had to react to by stating if, given the corresponding scenario, he would share his data. 78 responses were collected over a period of seven days. The results show a significant relationship for both consumer trust and transparency of data with willingness to share. Furthermore transparency of data shows to have a stronger effect on willingness to share than consumer trust. This study provides first insights into the antecedents of people's willingness to share private information for Internet of Things devices and creates a basis for further research of successful data collection methods in this industry.**

Supervisors: Dr. Rainer Harms
Dr. Efthymios Constantinides

Keywords
Internet of Things, Transparency, Consumer Trust, Data Collection, Data Security

7th IBA Bachelor Thesis Conference, July 1st, 2016, Enschede, The Netherlands.

1. INTRODUCTION

The term ‘Internet of Things’, in short ‘IoT’, plainly defined describes the connection of the Internet with physical things. Sensors are integrated in normal everyday devices, like a fridge, a car or a watch turning them into ‘smart objects’ that communicate and interact with each other as well as with human beings (Vermesan et al., 2011). Together, they are creating a dynamic global network of data and information promised to revolutionize business dynamics, social interaction and everyday life (Chui et al., 2010; Gubbi et al., 2013) An example of an Internet of Things device is the ‘Smart Meter’ by British Gas which is a small portable monitor measuring the energy consumption of a home and delivering this information via the Internet to the user as well as the energy provider in real time. The device is connected to all other households with a smart meter, which enables the user to compare his energy use with other households. This device creates a network of data about energy consumption and enables the provider British Gas and the user to accurately and easily track and compare the energy use of a whole country. This way, the device contributes to lower energy consumption by making people more aware about how much and in what way they actually use energy, contributing to a safer and greener future of the planet.

The Internet of Things is described as the new era of intelligence, developing into a new worldwide online ecosystem (Swan, 2012). Basically, it consists of data and information and completely depends on the accessibility of those (Gubbi et al., 2013). Since Internet of Things devices can be used in every sector of a human's life, sensible information is required to be shared, resulting into major privacy and security issues for the consumer (Sundareswaran et al., 2012):’One of the major challenges that must be overcome in order to push the Internet of Things into the real world is security’ (Roman et al., 2013, p. 2267). Achieving success when creating an Internet of Things device is determined by the consumers feeling secure enough to be willing to share their data. Identifying the drivers of people’s willingness to share data and their power of impact hence is crucial to the success and survival of the Internet of Things.

Several factors are found to be influencers of people’s feeling of security and their willingness to share data, however they show to be of different importance. Several researchers define accountability of data as an important factor of security (Weber, 2011; Benghabrit et al, 2015). The term relates to data being accessible, based on known sources and being used in a responsible way (Weber, 2011). Sundareswaran et al. (2012) emphasize the importance of accountability on the Internet to ensure privacy and security, especially in cloud computing. To tackle this issue, they developed a ‘cloud information accountability framework’ which enables consumers to access their data at all times and request security information when wanted. However, in many papers accountability is often related to transparency and even is handles as a potential consequence of transparency.

Several Internet of Things devices failed to take grip on the market due to consumers being unsure about what kind of information is being collected. A study in 2015 by the Ponemon Institute revealed that out of 1900 participants 82% stated that Internet of Things providers do not present any details about how their private data is used and handled. Transparency of data means knowing when, how and what kind of data is collected and being able to access the collected data (Awad & Krishnan, 2006; Turilli & Floridi, 2009). Not knowing how data is collected and where it is stored, hence creates fear among many consumers about lacking security, hindering the Internet of Things to really start off. Therefore, transparency of data is considered to be an important driving factor of willingness to share data and consequently of the success of the Internet of Things.

Literature shows that between two entities, in specific between a consumer and a company, trust is one of the main factors to ensure a successful and long-term relationship (Keen et al, 2000; Papadopoulou, 2006). Trust is commonly defined as knowing or believing that the trusted entity will not take advantage of oneself, hence feeling confident and secure with exposing one's vulnerability (Anette Baier, 1989). Since sharing sensible data is an act of exposing one’s vulnerability, several studies have been conducted and have identified trust as a central driving factor of sharing data on the Internet (McKnight et al., 2002; Teo & Liu, 2007). These studies have proven significance of consumer trust for people to share their data online, raising importance of consumer trust in Internet of Things devices.

The aforementioned outline can be concluded to the assumptions that consumer trust and transparency of data are crucial driving factors for people’s willingness to share data (Figure 1). As explained, accountability is considered to be similar to or even a consequence of transparency, making it too complicated to create a clear distinction of these two constructs in the research. Therefore, accountability is not being investigated as an antecedent of willingness to share data for an Internet of Things device in this paper and the focus will be put solely on transparency and consumer trust.

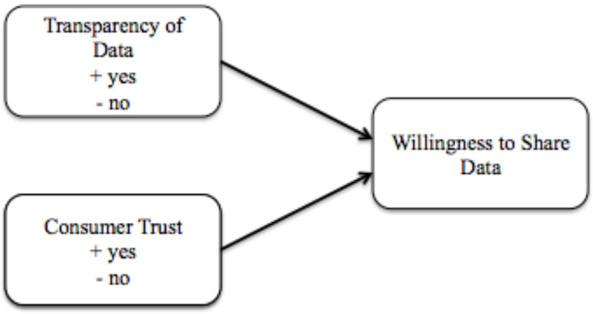


Figure 1

The relationship between transparency of data and willingness to share data and especially consumer trust and willingness to share data has been investigated several times and has proven to be significant. However, these studies all focused on sharing data on the Internet. Dwyer et al (2007) investigated the relationship between trust and willingness to share data on a social network site; a similar study was conducted by Shin (2010). Chellappa and Sin (2005) scrutinize the impact of consumer trust in an e-vendor and their willingness to share information for personalized advertising. Another study investigating willingness to share data for personalized advertising was made by Awad and Krishnan (2006) and Leon et al (2015), using transparency of data as a driving factor. Jin et al (2016) explored the impact of transparency of data collection on people’s acceptance of personalized advertising and therefore, also on the acceptance of letting companies collect private data. Willingness to transact with an e-vendor and share data and its relationship with trust was explored by several researchers (McKnight et al, 2002; Hoffman et al, 1999; Lwin et al, 2015).

The Internet of Things is a new phenomenon and making everyday objects, which have been in a person’s life for several years, the device that is collecting the data is potentially influencing a consumer’s way of thinking about sharing his data. When and how the data is collected is not as obvious to the consumer as on the common Internet and might result into scepticism towards the device. Trust therefore, might be of different importance to the consumer and requires a different approach from the company. Before creating new approaches of trust and transparency, it is important for a company to know if these factors are important and how powerful their influence is.

Considering these differences and the stated relevance for the future success of the Internet of Things domain, the following research question was created as the basis of the research presented in this paper.

Data Privacy and Internet of Things: How are Transparency of Data and Consumer Trust related to people's willingness to share data for an Internet of Things device?

This paper will contribute to existing literature by investigating the impact and the power of impact of transparency of data and consumer trust on willingness to share data not just on the Internet but for Internet of Things devices.

2. THEORETICAL SECTION

2.1 Transparency of Data

The term transparency can be used as the equivalent of 'see through' and is defined in two ways. In one of which it is an object; a see-through photograph printed on plastic made visible by shining light on it (Cambridge Dictionary, n.a.). Another definition, which is the basis for this paper, is describing transparency as a characteristic. Often the term is used as a synonym of openness and being clear and honest about one's operations (Ball, 2009). Within the topic of the Internet of Things transparency can be applied to data, in specific private data, hence as a customer having the ability to obtain information about who is collecting the data and how it is used (Awad & Krishnan, 2006). Transparency online has been defined by many researchers, however only few definitions focus on transparency of data specifically for Internet of Things devices.

Furthermore, transparency means making data accessible and visible (Zhu, 2002) as well as available to the customer (Turilli & Floridi, 2009). Honesty and reliability of the company as well as willingness to be open about the ways of collecting and using personal data are considered to be important characteristics of transparency in the Internet of Things sector (Hustvedt & Kang, 2013). An example of a transparency mechanism for data collection online is the 'opt-out rule' (the right to refuse) for the implementation of cookies. Cookies are a mechanism to track and carry personalized information of the user online and share the information with other websites, to enable personalized web experience in terms of advertising and searches. The opt-out rule was placed by law and was introduced by the European Data Protection Directive in order to enhance transparency and increase consumers' power over their own data online (Tene & Polenetsky, 2007). Although this is not a voluntarily placed mechanism by companies it enables consumers to achieve greater awareness about when and where data is collected and stimulates a more confident and positive attitude towards the website, hence the company. However, Tene and Polenetsky (2007) also criticise that most common transparency mechanisms consist of privacy policies, requiring the consumer to read pages of security claims, making it too complicated for the consumer to get informed. This way companies claim to be open about their data collection activities without actually offering transparency in forms of privacy practices.

Another perspective on transparency is presented by Turilli and Floridi (2009), who emphasize the ethical principles behind transparency of operations. Depending on the kind of information, e.g. safety facts, intentions of the company and usage of private data, ethical standards play an important role concerning the level of transparency. Turilli and Floridi (2009) elaborate on the ethical responsibility behind the factor transparency, meaning for certain information it would be ethically correct to be disclosed or to be concealed. Consequently, a company needs to be aware of the responsibilities that are attached to collecting information and handle the level of transparency accordingly. Disclosing or concealing certain information, hence implies great potential of damaging a company's reputation, image and business.

This perspective can be further developed towards transparency being a question about a person's rights (Elia, 2009). Birkinshaw (2006) even demands 'Freedom of Information' to be listed as a human right and counts transparency next to openness as a fundamental factor of freedom of information. As transparency on the one hand contains the right to receive information, on the other hand it also contains the right of privacy, meaning the right to withhold certain information (Weber, 2010).

Being open and clear about what kind of data is collected, for which purpose it is collected and where it is stored, therefore is a crucial factor in obtaining a successful data collection online and for Internet of Things devices.

2.2 Consumer Trust

The concept of trust is very ambiguous, many different definitions of the term exist, and some researches even decide not to define it at all (Benassi, 1999). Depending on the researcher's area of expertise, trust is seen as a different concept, e.g. a social construct, a personal trait or an economic choice mechanism (McKnight & Chervany, 2001). Throughout this paper, consumer trust will be handled as a social construct, an emotion a company is aiming to trigger in the customer. Trust has been known as an important antecedent for a successful interaction with the consumer and became even more important in the era of the Internet, due to a rise of uncertainty (Chellappa & Pavlou, 2002)

In the Internet of Things sector definitions of consumer trust rarely exist, however, the concept can be applied in a similar way as consumer trust online. In both settings, the consumer is confronted with a non-human mediator and is required to build trust based on the communication with an object, a device or a webpage (Mukherjee & Nath, 2007) without being able to rely on the information he receives from senses he would be able to use in an offline situation. Hence, the definition of consumer trust used as the basis of this paper is derived from definitions mostly focused on consumer trust online.

A very simple definition, a basic basis for the concept of trust, is the definition by philosopher Annette Baier (1989) which states that having trust in someone means giving the person an opportunity to harm oneself and believing he will not take it. Applying this concept to consumer trust online, it stresses the need for consumers to be confident about companies using their data responsibly to be able to build trust. Although in general, common definitions of trust can be applied to every situation, consumer trust online needs to be examined from a different perspective. In an offline setting, consumers can actually see, feel and talk with the entity asking for their trust and even can observe other people's reaction towards this entity. Online, all these senses are useless and the consumer has to rely on the information he is given at this moment by the company itself (McKnight & Chervany, 2001).

Building trust is an on-going, dynamic process that needs constant attention and work (Koufaris & Hampton-Sosa, 2004). A central factor to address when wanting to establish trust in the virtual world as well as in the real world is to build and retain a relationship with the customer (Keen et al, 1999; Papadopoulou, 2006). A relationship between a company and a customer online, next to other factors, is based on the technological capabilities, the expertise and the reputation of the company (Patokorpi & Kimppa, 2006). Several factors help to build trust and make a customer-company relationship grow stronger and last longer. One factor supporting trust building is when a promise that was made to the customer was enabled and kept by the company, resulting into a positive reputation also attracting other customers (Papadopoulou, 2006). Meeting a customer's expectation and keeping his best interest in mind are elements mentioned by several researchers as drivers of trust (Jaervenpaa et al., 1999; Gefen et al., 2003). In general, making the consumer feel secure and showing his well-being and consent is of major importance, is a crucial factor when trying to achieve trust in a relationship and further fosters a good reputation.

Several researchers emphasize reputation as one of the main drivers for consumer trust, especially in an online environment (Mukherjee & Nath, 2003; Chen & Barnes, 2007). Reputation is the result of previous interactions between consumers and the company and the consequential level of strengths of the brand (Egger, 2000). In their study about initial trust and online buying behaviour, Chen and Barnes (2007) find a significant relationship between initial trust online and reputation of the company, encouraging companies to adapt to customers' wishes and feedback. Consumers are known to rely on the advise of friends and family members when they are unsure if a certain company is trustworthy (Gentina & Bonsu, 2013; Bearden et al., 1989), in an online environment this becomes even more apparent due to the vast amount of products and brands available to the consumer (Dellarocas, 2004)

Another factor, which is commonly related to consumer trust, is risk (Kim et al., 2008). As mentioned in the second paragraph trust means giving a person the opportunity to harm oneself, hence taking the risk that another person or a company will take advantage of oneself (Gefen et al., 2003). Especially in the digital world, risk and uncertainty play important roles. Ensuring safety when sending financial or personal data is more complicated and requires much greater risk taking by the consumers in the digital world than offline (Lee & Turban, 2001). In their study Joinson et al (2010) found that the more sensitive the information is, the less willing people are to share it due to the implied risk. Sharing personal data can make consumers feel like they are losing privacy, hence risking financial and social loss (Zimmer et al., 2010). Therefore, reducing risk for the consumer and ensuring low uncertainty is considered to be a major determinant in building trust in a consumer-company relationship.

2.3 Transparency, Consumer Trust and Willingness to share data

The success of the Internet of Things industry is determined by people's willingness to provide sensitive and private information via a wireless connection with a company and other users. Many researchers investigated the antecedents of willingness to share data online and have identified several factors influencing a person's willingness to give private information on an online website (Leon et al., 2013). Several of these factors potentially can be applied to the Internet of Things; their direct effect however, has not yet been investigated.

Many researchers have explored the relationship between consumer trust online and willingness to share data, however with a focus on online shopping, hence consumers trust in e-commerce vendors. McKnight et al (2002) developed a trust building model based on antecedents of trust for e-vendors and investigated, next to several other drivers, the relationship between trust and willingness to share data with an e-vendor. The results show that there is a strong relationship between a consumer's trust in an e-vendor and his willingness to share personal information with the company. Therefore, it can be expected that in an Internet of Things setting consumer trust also has a great influence on willingness to share data and has the potential of increasing the success of a company's data collection.

Other than the relationship between consumer trust and willingness to share data, the relationship between transparency of data and willingness to share data has not been researched as much. In fact, many studies elaborate on the transparency of companies' web-presence, in specific their willingness to be open about their actions and operations and its effect on consumer's trust (Urban et al., 2009; Khan & Maluhi, 2010). Studies about consumers' attitude towards transparency of data and its influence on a consumer's willingness to reveal sensitive information are lacking. However, an example of a study about transparency of data was executed by Awad and Krishnan (2006). They investigated if consumers, rating transparency of data being important, are less willing to be profiled online for personalized advertising than consumers rating transparency of data as non-important. The study reveals that the relationship is significant which emphasizes the importance of the factor data transparency in achieving a successful collection of personal data from consumers.

Internet of Things is a steadily growing industry; its wide area of application and its easy and handy way of use makes it being one of the most promising industries of the future (Atzori & Morabito, 2010; Zhang et al., 2015). As the Internet of Things consists of data; collecting and obtaining data is one of the main activities in the IoT world (Caron et al., 2016). Knowing how to obtain the data one needs therefore is a key point in a company's strategy. It is assumed that transparency of data and consumer trust are one of the main drivers of consumer's willingness to share data. Therefore the following hypotheses will be investigated:

H1: Transparency of data increases consumer's willingness to share their data

H2: Consumer's trust increases consumer's willingness to share their data

3. METHODOLOGY

3.1 Sample

To explore the stated hypotheses, research in form of a vignette survey will be conducted. The survey consists of 4 scenarios each followed by one statement. It was created via Google Forms and was spread mostly via Facebook and Mail. In total seven questions were asked, three general questions and four questions to measure the independent variable. To increase quality and quantity of responses, the survey was conducted semi-anonymously, meaning the respondents are mostly friends and acquaintances of the researcher and were contacted via Mail and Facebook. However, names of participants will not be published. Since the research is about sharing personal data, the focus will be on any person having access to Internet and being older than the age of 18, as the common age in Europe at which people legally are fully responsible for themselves and the decisions they make is 18.

A G*Power test revealed that to achieve a power level of 95, 73 responses need to be collected, which means that if there is an effect, with 73 responses one can be 95% sure to be able to detect this effect. Therefore, 73 responses were set to be the minimum target number to be collected by asking friends and acquaintances. Since this did not result into enough responses in the given time, friends were asked to send the survey to their friends and acquaintances. With this trade-off it was possible to receive 78 responses over a period of one week. However, as a result of this method it was not possible to detect a response rate, since it is not clear to how many people the survey was actually sent.

3.2 Operationalization

A vignette survey includes a certain number of scenarios about a hypothetical situation or character, which the respondent needs to react to by choosing one of the given hypothetical actions (Finch, 1987). Using common questionnaires require the respondent to create his own mental picture of the hypothetical situation at hand, resulting into possible biased and unreliable answers. Furthermore questions presented to the respondent are often too abstract to be able to apply responses to the actual research problem (Alexander & Becker, 1978). To avoid this bias and to ensure respondents apply their answers to an Internet of Things device, a vignette survey method was chosen. With this method the respondent is presented a detailed and specific scenario, to which he can react accordingly.

The first three questions in the survey are to check the variety of respondents concerning nationality, gender and age to increase the ability to generalize the responses. In the next section, the respondent needs to read a short story about the history and functioning of the application 'Smart Meters'. Following this section 4 different scenarios are presented, each applying both independent variables Transparency and Consumer Trust to the short story as either 'positive' or 'negative'. This results into 4 different combinations of the independent variables with each other.

Dependent Variable: Willingness to share data

The dependent variable 'Willingness to share data' is measured via one item. After each scenario the participant is asked to respond to the following statement "For the application 'Smart Meters', I am willing to share my data" with a dichotomous response: 'Yes' or 'No'. The dependent variable 'willingness to share data' is measured via the answers of the statement.

Independent Variables: Transparency of Data & Consumer Trust

The characteristics of Transparency represented in the scenarios are derived from questions developed by Awad and Kreshnan (2006). Awad and Kreshnan (2009) originally measured 'Information Transparency' by asking respondents about the level of importance of four characteristics of Transparency. Since this research uses a vignette-survey and the independent variables are measured using a scenario, the items of Awad and Kreshnan (2009) were transformed into statements. The same procedure was applied to the four items concerning consumer trust online developed by Teo and Liu (2007). Teo and Liu (2007) originally presented five items about consumer trust online to the respondent, however one item was directly asking to state if the presented company was trustworthy. The vignette survey is used to confront the respondent with a description of an application to find out if, in the given situation, his trust in the application would be great enough to share his data. Since consumer trust is an independent variable, using this statement would require labelling the application as trustworthy in the scenario, hindering the respondent to make up his own mind about the company's level of trustworthiness. Therefore, this statement will not be used for the research of this paper. As a substitution, a new statement was created, based on the definitions from the theory part of this paper: "I know the company will not use my data at my disadvantage". These measurements are considered to be reliable since the related article by Awad and Kreshnan (2009) and Teo and Liu (2007), were cited 484 times and 403 times accordingly. See the appendix for the whole survey.

Control Variables

To further assess the relationship between transparency of data, consumer trust and willingness to share data, control variables are added. Age and gender are inserted as control variables, since they might have an effect on the relationship between the independent variables and the dependent variable. Nationality is not included as a control variable since the spread based on continents is not great enough.

3.3 Method of Analysis

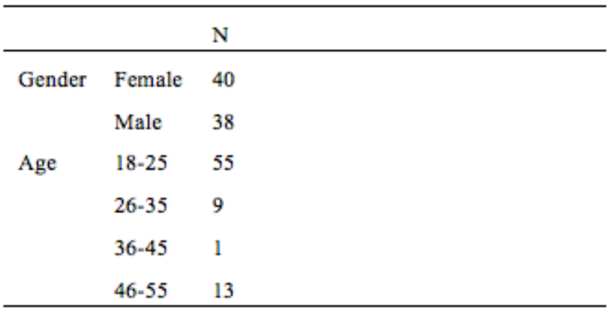
78 responses were collected during a timeframe of 7 days; all of the responses were valid and could be used for further investigation. Descriptive statistics were first to be analysed. The main analysis was conducted via a general linear model with repeated measures. First the results of the multivariate analysis will be examined to detect if a significant relationship exists. Furthermore the effect of the control variables will be analysed and their impact on the relationship. In the second step we will investigate the strength of the relationships between the two independent variables and the dependent variable to conclude which independent variables has a greater impact on the dependent variable. These analyses were chosen because we have two explanatory variables and one related outcome variable. Throughout the analysis an α of .05 is used.

4. RESULTS

4.1 Descriptive Statistics

Table 1 shows an overview of the descriptive statistics, consisting of the gender and the age of the respondents. Furthermore the nationalities of the respondents were examined. Out of the 78 respondents 40 were female and 38 were male. The age group of 18-25 is the biggest with 55 respondents and the age group of 36-45 is the smallest with only one respondent.

Table 1: Descriptive Statistics



		N
Gender	Female	40
	Male	38
Age	18-25	55
	26-35	9
	36-45	1
	46-55	13

The nationalities of the respondents is spread over 3 continents, with most of them originating from Europe, 2 from Australia and 5 from Central America. Germans represent the biggest nationality with 48 respondents, followed by the Dutch with 17 respondents.

4.2 Main Analysis

In the following section the findings of the main analysis, the outcome of the multivariate test is described.

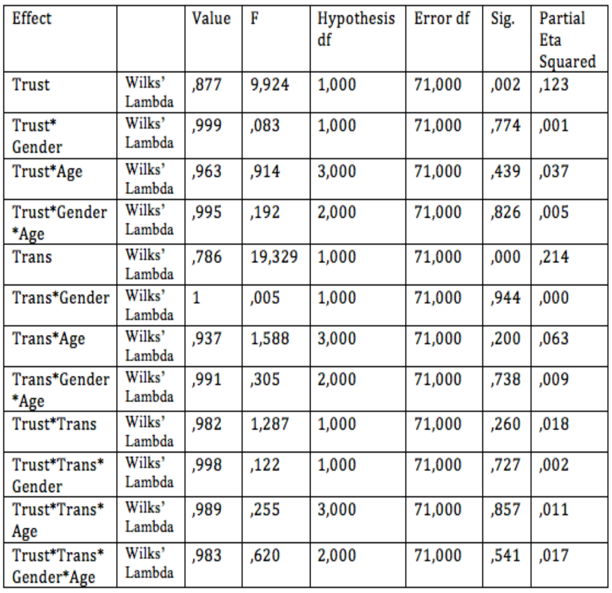
Table 2 shows the most important outcome of the multivariate test of the independent variables consumer trust and transparency of data on the dependent variable. Also, it includes the control variables GENDER and AGE.

Transparency of data was found to have a statistically significant main effect on willingness to share data (Wilks' Lambda = 0.79; F(1,71) = 19.33; p<0.05; Partial Eta Squared = .21) To determine the direction of the main effect, a 95% confidence interval was conducted. The confidence interval revealed that positive transparency of data has a greater effect on people's willingness to share data than negative transparency of data; meaning when transparency of data exists, people are more willing to share their data (95%CI = [-.21; -.51]). Therefore hypothesis *H1: "Transparency of data increases consumer's willingness to share data"* is proven to be statistically significant and has to be accepted.

Consumer trust was found to have a statistically significant main effect on willingness to share data (Wilk's Lambda = 0.88; F(1,71) = 9.92; p<0.05; Partial Eta Squared = .12). To determine the direction of the main effect, a 95% confidence interval was conducted. The confidence interval revealed that positive consumer trust has a greater effect on people's willingness to share their data than negative consumer trust; meaning when consumer trust exists, people are more willing to share their data (95%CI = [-.15; -.47]). Therefore hypothesis *H2: "Consumer trust increases consumer's willingness to share their data"* is proven to be statistically significant and has to be accepted.

For further investigation the effect of the control variables age and gender were examined. The control variable AGE does not show any statistically significant effect on Trust (Wilks' Lambda = 0.973; F(3,71) = .94; p= .44) nor on Transparency (Wilks' Lambda = .937; F(3,71) = 1.59; p=.2). The control variable GENDER does not show any statistically significant effect on Trust (Wilks' Lambda = 1; F(1,71) = .08; p= .77) nor on Transparency (Wilks'Lambda = 1; F(1,71)= .005; p=.94).

Table 2: Multivariate Analysis of Consumer Trust and Transparency of Data



Effect		Value	F	Hypothesis df	Error df	Sig.	Partial Eta Squared
Trust	Wilks' Lambda	,877	9,924	1,000	71,000	,002	,123
Trust* Gender	Wilks' Lambda	,999	,083	1,000	71,000	,774	,001
Trust*Age	Wilks' Lambda	,963	,914	3,000	71,000	,439	,037
Trust*Gender *Age	Wilks' Lambda	,995	,192	2,000	71,000	,826	,005
Trans	Wilks' Lambda	,786	19,329	1,000	71,000	,000	,214
Trans*Gender	Wilks' Lambda	1	,005	1,000	71,000	,944	,000
Trans*Age	Wilks' Lambda	,937	1,588	3,000	71,000	,200	,063
Trans*Gender *Age	Wilks' Lambda	,991	,305	2,000	71,000	,738	,009
Trust*Trans	Wilks' Lambda	,982	1,287	1,000	71,000	,260	,018
Trust*Trans* Gender	Wilks' Lambda	,998	,122	1,000	71,000	,727	,002
Trust*Trans* Age	Wilks' Lambda	,989	,255	3,000	71,000	,857	,011
Trust*Trans* Gender*Age	Wilks' Lambda	,983	,620	2,000	71,000	,541	,017

Furthermore it is interesting to see how great the effects of the independent variables are on the dependent variable. This can be concluded via the partial eta squared. The scale of magnitude for the Partial Eta Squared developed by Cohen (1988) describes a rule of thumb for the size of the effect. A partial eta squared of .01 is considered to be small, of .06 is medium and .14 is big. Considering this scale, table 2 shows that both independent variables have a strong effect on the dependent variable. Furthermore one can conclude from the analysis that transparency of data (Partial Eta Squared =.214) has a greater effect on willingness to share data than consumer trust (Partial Eta Squared =.123).

Also, table 2 displays the interaction effect between the two independent variables. The results show that there is no statistically significant interaction effect between transparency of data and consumer trust (Wilk's Lambda = 0.982; F(1,71) = 1.29; p=.26; Partial Eta Squared = .08). Therefore, a pairwise comparison becomes irrelevant.

5. DISCUSSION

The research in this paper was conducted to answer the following research question: *Data Privacy and Internet of Things: How are Transparency of Data and Consumer Trust related to people's willingness to share data for an Internet of Things device?* Considering the findings, it can be said that there is a clear positive relationship between consumer trust and willingness to share data as well as between transparency of data and willingness to share data.

Furthermore it is interesting to see, that transparency of data has a greater positive effect on willingness to share data than consumer trust, putting greater importance on making the data collection more transparent than developing consumer trust.

Both of these findings create an important basis for future data collection and company-consumer relationship building methods online and in specific for Internet of Things devices. Data privacy is one of the main issues that Internet of Things companies need to face and especially the consequential lack of willingness to share data from the consumers. Knowing that transparency of data and consumer trust have such a significant effect on people's willingness to share data opens up opportunities of improvements of the devices themselves as well as for how to approach the consumer with an Internet of Things device concerning marketing and usage.

Clearly and obviously presented privacy and security statements form the company that are accessible easily and at all times for the user may already foster the success of Internet of Things devices. Miorandi et al (2012) emphasized in their paper the lack of privacy and security and in specific the lack of mechanisms ensuring these features to the consumer, being the crucial factor to hinder the Internet of Things' further development. Transparency of data does not represent the privacy mechanism itself, but indicates a great step towards greater privacy and security. Opening up about ones data collection methods and enabling access and visibility of data at all times for the consumer naturally forces the company to implement safety and privacy mechanisms, otherwise loosing customers.

An example of a company failing to be transparent about its data collection is Google. In specific, Google failed to be honest about what kind of data is collected. In order to revolutionize its online applications GoogleEarth and GoogleMaps with the newest feature Google Street View, cars equipped with cameras drove through the world's cities and captured every street and every house in panoramic pictures. Although during the process it was meant for Google to only take pictures of the streets, it was revealed in 2010, that the cars also have been collecting private data from Wi-Fi networks. Unknown before to anyone outside of Google, this revealment developed into a worldwide scandal and caused great fines for Google in Australia, Germany and the United States. More importantly, Google's reputation was damaged. Stakeholders now naturally take a closer look on security issues and approach the brand Google in a more careful way.

Looking at the Google Street View scandal it becomes clear how severe the consequences can be. Especially for smaller and younger companies, not being honest about the data collection method and not providing transparent data may result into viability problems. Adding the findings of this research, it becomes clear that transparency of data is not only a factor of interest for the consumer but also for the company itself.

As found in this research, transparency of data is more important to a successful collection of data than consumer trust. An assumption for the reason of this outcome is connected to several researchers investigating transparency as a driver of trust online (Pollach, 2005; Duranti & Rogers, 2016). If transparency of data exists, the consumer receives a comprehensive insight into the practices of the company concerning data handling and information storage. Consequentially, the consumer knows that is data is handled responsibly and that he, as a consumer, is treated with respect, automatically leading to consumer trust, which decreases the importance of trust mechanisms and increases the importance of transparency mechanisms.

However, the results show that there is no interaction effect between transparency of data and consumer trust, meaning that the nature or strength of relationship between one independent variable and the dependent variable does not change as function of the other independent variable. Therefore, the assumption made above is not supported, since increased transparency of data does not influence the relationship between consumer trust and willingness to share for this Internet of Things device.

Another assumption for the reason for transparency of data having greater strength than consumer trust is that building trust takes time (Lindenberg, 2000). The respondent was presented with a company described as trustworthy however, he does not actually know the company and needs to decide, based on few information and within a few minutes, if he perceives this company as trustworthy. As a consequence, the respondent potentially perceives the level of transparency in the given scenarios as being higher than the level of trust, therefore, rating transparency as the greater driver to their willingness to share personal data.

Google is a big company with many successful products and applications and has a substantial amount of long-term customers that put great trust in the brand Google. Although, Google had to face many fines and showed great lack of transparency, the company did not suffer any severe losses and customers still chose Google over many other brands and are willing to share sensible information. This contradicts to the results of this study, which rates transparency of data having a greater impact than consumer trust. However, this contradiction supports the assumption made above that trust built over a long period of time develops into a stronger driver of willingness to share than transparency of data.

When looking at the Internet of Things device used as an example in the survey, Smart Meters, enhancing transparency of data and consumer trust are valuable actions for the company to make. Derived from the statements used in the scenarios and the reactions of the respondents towards those, certain points are revealed for how to increase both variables for the device at hand.

To enhance consumer trust, Smart Meters needs to make sure to have a reliable and available customer service to be ready to help with any problems the customer might encounter with the Smart Meters device. Furthermore trust is enhanced, when the customer feels respected and his personal information treated responsibly. This can be achieved by communicating and ensuring an extensive data safety policy for Smart Meters and keeping the promises made in the policy. Furthermore, this can be communicated in the customer service by treating the customer with respect and ensuring problems and issues are dealt with immediately and extensively. Making the consumer confident, his information will not be used to his disadvantage, by proving detailed information about how and from whom the data will be used is not just enhancing consumer trust but also transparency of data.

Transparency of data can be increased when the customer is explained pre-purchase that only data about his energy use and his payment information will be collected and saved from him. Furthermore providing an online platform which the customer has access to at any given time and on which he can check and eventually delete the data that was collected from him, is a great tool of providing transparency. In this online platform the company can post frequent updates about how and for what purpose the customer's data was used, when and for what reason certain data is deleted and in what way his energy consumption might have contributed to an overall greener environment.

The Internet of Things is considered to be one of the biggest, if not the biggest upcoming trend of the future. Research has shown that privacy and security issues are one of the main reasons for the Internet of Things to not yet fully start off. Since it is based on data, knowing what factors are crucial to consumers to be willing to share their data with Internet of Things companies therefore is one of the main success factors for this trend and of major importance for its further development.

6. LIMITATIONS & FURTHER RESEARCH

Although this study was to investigate the influence of transparency of data and consumer trust on willingness to share data for Internet of Things devices in general, the vignette survey method provides the respondent with information about a specific Internet of Things device and is asked to respond to the given scenario. Therefore, the results can be only reliably applied to this device or other Internet of Things devices collecting similar kind of data from the consumer. Devices requiring the consumer to share more private and more intimate data might obtain different or weaker results.

Another limitation is the number of respondents. Although a set of 78 responses is enough to obtain a valid outcome, a greater number is necessary to be able to apply the results to a whole population. A variety in age and nationalities as well as an even spread of women and men makes the study generalizable but does not enable to investigate specific groups like women in the age of 25-45 or only Dutch people.

A critic that could be made is the method of data collection. Since friends of friends and family asked, trustworthiness of the answers cannot be ensured. Also it can be criticized that the collection of data was biased by choosing respondents that fit best to the assumptions made by the researcher since the respondents mostly were friends and acquaintances.

Furthermore, as presented as a potential explanation for the outcome of this study, consumer trust might be biased since the respondent was not offered the necessary time and information to develop a solid amount of trust towards the company. Choosing a company known to the respondent and that he already trusts beforehand as the trustworthy entity in the scenarios might show different results.

Also, pre-experiences of the respondent with data privacy and security issues were not taken into consideration. Respondents who had an extremely bad or an extremely good experience with online data security might rate transparency of data and consumer trust differently on a scale of importance and would react differently to the given scenarios than respondents who have not encountered any security issues online.

This study revealed that consumer trust and transparency of data are crucial factors increasing the amount of people sharing their data, however it does not elaborate on how to increase these two factors. Investigating what are the drivers of consumer trust and the drivers of transparency of data are possible points for further research in this domain. Furthermore, since transparency of data and consumer trust have a different size of effect on willingness to share data, it can be interesting to see if these differences change when company and device characteristics are considered.

Other points of research are further factors influencing willingness to share data. Due to a lack of time only transparency of data and consumer trust have been investigated as driving factors of people's willingness to share data, however there are several other potential factors having major or minor influences on willingness to share and people's feeling of security.

7. ACKNOWLEDGEMENTS

I would like to thank my first supervisor Dr. Rainer Harms for his ideas and knowledge input in writing this thesis, as well I would like to thank my second supervisor Dr. Efthymios Constantinides and my fellow peer reviewers. Finally I want to thank my family and all my friends for supporting me throughout this process and for participating in my research.

8. REFERENCES

Alexander, C. S., & Becker, H. J. (1978). The use of vignettes in survey research. *Public opinion quarterly*, *42*(1), 93-104.

Anette Baier, A. (1986). Trust and antitrust. *Ethics*, *96*(2), 231-260.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks*, *54*(15), 2787-2805.

Awad, N. F., & Krishnan, M. S.. (2006). The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization. *MIS Quarterly*, *30*(1), 13–28.

Ball, C. (2009). What Is Transparency? *Public Integrity, 11*(4), 293-308. doi:10.2753/pin1099-9922110400

Bearden, W. O., Netemeyer, R. G., & Teel, J. E. (1989). Measurement of consumer susceptibility to interpersonal influence. *Journal of consumer research*, 473-481.

Benassi, P. (1999). TRUSTe: An online privacy seal program. *Communications of the ACM Commun. ACM, 42*(2), 56-59. doi:10.1145/293411.293461

Benghabrit, W., Grall, H., Royer, J., Sellami, M., Azraoui, M., Elkhiyaoui, K.., Bernsmed, K. (2015). From Regulatory Obligations to Enforceable Accountability Policies in the Cloud. Communications in Computer and Information Science Cloud Computing and Services Sciences, 134-150. doi:10.1007/978-3-319-25414-2_9

Birkinshaw, P. (2006). Freedom of information and openness: Fundamental human rights?. *Administrative Law Review*, 177-218.

Caron, X., Bosua, R., Maynard, S. B., & Ahmad, A. (2016). The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective. *Computer Law & Security Review, 32*(1), 4-15. doi:10.1016/j.clsr.2015.12.001

Chellappa, R. K., & Pavlou, P. A. (2002). Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management*, *15*(5/6), 358-368.

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management*, *6*(2-3), 181-202.

Chen, Y. H., & Barnes, S. (2007). Initial trust and online buyer behaviour. *Industrial management & data systems*, *107*(1), 21-36.

Chui, M., Löffler, M., & Roberts, R. (2010). The internet of things. *McKinsey Quarterly*, *2*(2010), 1-9.

Ponemon Institute LLC. (2015, February 19). *Internet of Things: Connected Life Security.* United States.

Cohen, J. (1988). Statistical Power Analysis for the Behavioral Sciences. 2nd edn. Hillsdale, New Jersey: L.

Dellarocas, C. (2004). Building trust online: The design of robust reputation. *Social and economic transformation in the digital era*, 95.

Duranti, L., & Rogers, C. (2016). Trust in Records and Data Online. *Integrity in Government through Records Management. Essays in Honour of Anne Thurston*, 203-214.

Dwyer, C., Hiltz, S., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. *AMCIS 2007 proceedings*, 339.

Egger, F.N. (2000), Towards a model of trust for e-commerce system design. Working paper, IPO, Center for User-System Interaction, Eindhoven University of Technology.

Elia, J. (2009). Transparency rights, technology, and trust. *Ethics and Information Technology Ethics Inf Technol, 11*(2), 145-153. doi:10.1007/s10676-009-9192-z

Finch, J. (1987). The vignette technique in survey research. *Sociology*, 105-114.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: an integrated model. *MIS quarterly*, *27*(1), 51-90.

Gentina, E., & Bonsu, S. K. (2013). Peer network position and shopping behavior among adolescents. *Journal of Retailing and Consumer Services*, *20*(1), 87-93.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645-1660.

Hoffman, D. L., Novak, T. P., & Peralta, M. (1999). Building consumer trust online. *Communications of the ACM Commun.* ACM, 42(4), 80-85. doi:10.1145/299157.299175

Hustvedt, G., & Kang, J. (2013). Consumer Perceptions of Transparency: A Scale Development and Validation. *Family and Consumer Sciences Research Journal* Fam Consum Sci Res J, 41(3), 299-313. doi:10.1111/fcsr.12016

Jarvenpaa, S. L., Tractinsky, N., & Saarinen, L. (1999). Consumer Trust in an Internet Store: A Cross-Cultural Validation. *Computer-Mediated Communication,5*(2). doi:0.1111/j.1083-6101.1999.tb00337.x

Jin, Y., Seipp, K., Duval, E., & Verbert, K. (2016, June). Go With the Flow: Effects of Transparency and User Control on Targeted Advertising Using Flow Charts. In *Proceedings of the International Working Conference on Advanced Visual Interfaces* (pp. 68-75). ACM.

Joinson, A. N., Reips, U. D., Buchanan, T., & Schofield, C. B. P. (2010). Privacy, trust, and self-disclosure online. *Human–Computer Interaction*, *25*(1), 1-24.

Keen, P., Ballance, G., Chan, S., & Schrump, S. (1999). *Electronic commerce relationships: Trust by design*. Prentice Hall PTR.

Khan, K. M., & Malluhi, Q. (2010). Establishing trust in cloud computing. *IT professional*, *12*(5), 20-27.

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems, 44*(2), 544-564. doi:10.1016/j.dss.2007.07.001

Koufaris, M., & Hampton-Sosa, W. (2004). The development of initial trust in an online company by new customers. *Information & management*, *41*(3), 377-397.

Lee, M. K., & Turban, E. (2001). A trust model for consumer internet shopping. *International Journal of electronic commerce*, *6*(1), 75-91.

Leon, P. G., Rao, A., Schaub, F., Marsh, A., Cranor, L. F., & Sadeh, N. (2015). *Why people are (Un) willing to share information with online advertisers*. Technical Report CMU-ISR-15-106, Carnegie Mellon University.

Leon, P. G., Ur, B., Wang, Y., Sleeper, M., Balebako, R., Shay, R., ... & Cranor, L. F. (2013, July). What matters to users?: factors that affect users' willingness to share information with online advertisers. In *Proceedings of the ninth symposium on usable privacy and security* (p. 7). ACM.

Lindenberg, S. (2000). It takes both trust and lack of mistrust: The workings of cooperation and relational signaling in contractual relationships. *Journal of management and governance*, *4*(1), 11-33.

Lwin, M., Wirtz, J., & Stanaland, A. J. (2015). The Privacy Dyad: Antecedents of Promotion-and Prevention-Focused Online Privacy Behaviors and the Mediating Role of Trust and Privacy Concern.

McKnight, D. H. & Chervnay, N. L. (2001). What trust means in -commerce customer relationships: an interdisciplinary conceptual typology. *International journal of electronic commerce*, *6*(2), 35-59.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). The impact of initial consumer trust on intentions to transact with a web site: a trust building model. *The Journal of Strategic Information Systems*, *11*(3), 297-323.

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, *10*(7), 1497-1516.

Mukherjee, A., & Nath, P. (2007). Role of electronic trust in online retailing: A re-examination of the commitment-trust theory. *European Journal of Marketing*, *41*(9/10), 1173-1202.

Mukherjee, A., & Nath, P. (2003). A model of trust in online relationship banking. *International Journal of Bank Marketing*, *21*(1), 5-15.

Papadopoulou, P., Andreou, A., Kanellis, P., & Martakos, D. (2001). Trust and relationship building in electronic commerce. *Internet Research, 11*(4), 322-332. doi:10.1108/10662240110402777

Patokorpi, E., & Kimppa, K. K. (2006). Dynamics of the key elements of consumer trust building online. *J of Inf, Com & Eth in Society Journal of Information, Communication and Ethics in Society, 4*(1), 17-26. doi:10.1108/14779960680000278

Pollach, I. (2005). A typology of communicative strategies in online privacy policies: Ethics, power and informed consent. *Journal of Business Ethics*, *62*(3), 221-235.

Shin, D. H. (2010). The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *Interacting with computers*, *22*(5), 428-438.

Sundareswaran, S., Squicciarini, A. C., & Lin, D. (2012). Ensuring distributed accountability for data sharing in the cloud. *Dependable and Secure Computing, IEEE Transactions on*, *9*(4), 556-568.

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, *57*(10), 2266-2279. (p. 2267)

Swan, M. (2012). Sensor mania! the internet of things, wearable computing, objective metrics, and the quantified self 2.0. *Journal of Sensor and Actuator Networks*, *1*(3), 217-253.

Tene, O., & Polenetsky, J. (2012). To Track or Do Not Track: Advancing Transparency and Individual Control in Online Behavioral Advertising. *Minn. JL Sci. & Tech.*, *13*, 281.

Teo, T. S., & Liu, J. (2007). Consumer trust in e-commerce in the United States, Singapore and China. *Omega*, *35*(1), 22-38.

Transparency Meaning in the Cambridge English Dictionary. (n.d.). Retrieved April 30, 2016, from http://dictionary.cambridge.org/dictionary/english/transparency

Turilli, M., & Floridi, L. (2009). The ethics of information transparency. *Ethics and Information Technology Ethics Inf Technol, 11*(2), 105-112. doi:10.1007/s10676-009-9187-9

Urban, G. L., Amyx, C., & Lorenzon, A. (2009). Online trust: state of the art, new frontiers, and research potential. *Journal of Interactive Marketing*, *23*(2), 179-190.

Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., ... & Doody, P. (2011). Internet of things strategic research roadmap. *Internet of Things-Global Technological and Societal Trends*, 9-52.

Weber, R. H. (2011). Accountability in the Internet of Things. *Computer Law & Security Review, 27*(2), 133-138. doi:10.1016/j.clsr.2011.01.005

Weber, R. H. (2010). Internet of Things–New security and privacy challenges. *Computer Law & Security Review*, *26*(1), 23-30.

Zhang, Y., Zhang, G., Wang, J., Sun, S., Si, S., & Yang, T. (2015). Real-time information capturing and integration framework of the internet of manufacturing things. *International Journal of Computer Integrated Manufacturing*, *28*(8), 811-822.

Zhu, K. (2002). Information Transparency in Electronic Marketplaces: Why Data Transparency May Hinder the Adoption of B2B Exchanges. *Electronic Markets,12*(2), 92-99. doi:10.1080/10196780252844535

Zimmer, J. C., Arsal, R. E., Al-Marzouq, M., & Grover, V. (2010). Investigating online information disclosure: Effects of information relevance, trust and risk. *Information & Management*, *47*(2), 115-123.

9. APPENDIX

9.1 Scenario with positive consumer trust and negative transparency of data

Peter has had the Smart Meters application now for about 8 months and as promised beforehand accessing his data is very simple which has made his daily life easier and him more aware of how much energy he uses. Also every time he is not sure about something concerning how to use certain data and where to find it and he sends an email to the company with questions, their answers always are very helpful and reliable. He really feels like they are keeping his best interest in mind by using his data responsibly and are trying to meet his expectations about secure data use. He is sure none of the data they receive from him will be used to his disadvantage. Concerning the data that is send to the company through the application he actually does not know what kind of information they are saving and if he could find out. Except to send him bills, he does not know for which purpose the company uses his information and for how long they will keep it. Neither is he sure if the data represents himself in a right way.

9.2 Scenario with negative consumer trust and negative transparency of data

Peter has had the Smart Meters application now for about 8 months and, although that is what they promised, accessing his data is rather complicated and he still does not really know how much energy he uses. Also every time he is not sure about how to access or use his data and he sends an email to the company with questions, their answers are vague and not really helpful. He feels like they do not really care about him as a customer and the expectations he had of the company concerning secure data use are not fulfilled. He is unsure if the company will not use his data to his disadvantage. Concerning the data that is send to them through the application he actually does not know what kind of information they are saving and if he could find out. Except to send him bills, he does not know for which purpose the company uses his information and for how long they will keep it. Neither is he sure if the data represents himself in a right way.

9.3 Scenario with negative consumer trust and positive transparency of data

Peter has had the Smart Meters application now for about 8 months and, although that is what they promised, accessing his data is rather complicated and he still does not really know how much energy he uses. Also every time he is not sure about how to access or use his data and he sends an email to the company with questions, their answers are vague and not really helpful. He feels like they do not really care about him as a customer and the expectations he had of the company concerning secure data use are not fulfilled. He is unsure if the company will not use his data to his disadvantage. Concerning the information they are collecting from him through the application he actually knows exactly what kind of data they are saving and that he can access it online through the website's company to check all the data they collected about him. They have explained him that all the data is saved for 10 years and then it is deleted. Furthermore he knows that they collect the data to have an accurate representation of his and the country's energy use and to improve their marketing and customer care. Peter is confident the collected data identifies him in a right way.

9.4 Scenario with positive consumer trust and positive transparency of data

Peter has had the Smart Meters application now for about 8 months and as promised beforehand accessing his data is very simple which has made his daily life easier and him more aware of how much energy he uses. Also every time he is not sure about something concerning how to use certain data and where to find it and he sends an email to the company with questions, their answers always are very helpful and reliable. He really feels like they are keeping his best interest in mind by using his data responsibly and are trying to meet his expectations about secure data use. He is sure none of the data they receive from him will be used to his disadvantage. Concerning the information they are collecting from him through the application he actually knows exactly what kind of data they are saving and that he can access it online through the website's company to check all the data they collected about him. They have explained him that all the data is saved for 10 years and then it is deleted. Furthermore he knows that they collect the data to have an accurate representation of his and the country's energy use and to improve their marketing and customer care. Peter is confident the collected data identifies him in a right way.

9.5 Statement used after each scenario to determine Willingness to share data

1) For application 'Smart Meters' I am willing to share my data