Investigating the effect of security and privacy on IoT device purchase behaviour

Ho-Sam-Sooi, Nick; Pieters, Wolter; Kroesen, Maarten

DOI
10.1016/j.cose.2020.102132

Publication date
2021

Document Version
Final published version

Published in
Computers and Security

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Investigating the effect of security and privacy on IoT device purchase behaviour

Nick Ho-Sam-Sooi, Wolter Pieters, Maarten Kroesen*

Delft University of Technology: Faculty of Technology, Policy and Management, P.O. Box 5015, 2600 GA Delft, Netherlands

ARTICLE INFO

Article history:
Received 8 July 2020
Revised 5 November 2020
Accepted 29 November 2020
Available online 3 December 2020

Keywords:
Purchasing behaviour
Security
Privacy
IoT
Public policy
Choice modelling

ABSTRACT

Given the significant privacy and security risks of Internet-of-Things (IoT) devices, it seems desirable to nudge consumers towards buying more secure devices and taking privacy into account in the purchase decision. In order to support this goal, this study examines the effect of security and privacy on IoT device purchase behaviour and assesses whether these effects are sensitive to framing, using a mixed methods approach. The first part of the study focuses on quantifying the effect of security and privacy compared to the effect of other device attributes such as price or functionality, by testing a causal model with choice models that have been developed from stated choice data. The second part aims to reveal the underlying mechanisms that determine the effect of privacy and security on purchase behaviour by means of a qualitative survey. The results suggest that security and privacy can strongly affect purchase behaviour, under the circumstances that privacy- and security-related information is available and communicated in an understandable manner, allowing consumers to compare devices. Moreover, the results show that a description of security that focuses on gains is more effective in nudging consumers towards buying secure devices. Future efforts could build upon this study by comparing the effect of security and privacy to more device attributes, such as ease of use or cost reduction. The results can serve as a basis for interventions that nudge consumers towards buying more secure and privacy-friendly devices.

1. Introduction

In the Internet-of-Things (IoT), physical objects are connected to a network via internet connectivity to deliver a service to a user (Sicari et al., 2015; Singh and Kapoor, 2017). The market penetration and societal acceptance of IoT devices is ever-increasing, as more and more use cases for the devices arise and the affordability of the devices improves. This trend is supported by the development of 5G network technology, which allows for lower latency connections and enables larger volume traffic, thus vastly improving the quality of services provided by IoT devices. IoT devices can provide significant value to consumers by enabling new functionalities that improve their quality of life. For example, smart thermostats enable consumers to remotely configure the heating in their home or even remove the need for manual adjustment of their heating system completely.

Although the adoption of IoT devices has significant benefits for consumers, it also introduces some notable risks with

* Corresponding author.
E-mail address: w.pieters@tudelft.nl (W. Pieters).
https://doi.org/10.1016/j.cose.2020.102132

regard to security and privacy. In many cases, IoT devices have inadequate basic security controls such as encryption or authentication schemes. Moreover, manufacturers collect large amounts of highly sensitive personal information, such as energy use data. When such data is shared with external third parties, an intentional or malicious infringement of the device owner's privacy might occur.

Consumers – both individual and business users – can play a large role in mitigating these risks, for example by purchasing secure devices and taking privacy into account when purchasing a device. If consumers value security and privacy, and are able to distinguish secure from insecure devices, they are willing to pay for added security. Manufacturers then have an incentive to improve the security of their products, increasing the overall security in the IoT ecosystem. However, both individual consumers and small companies often do not have the required technical knowledge to assess the security level of a device. Moreover, communication of privacy information is often lengthy and overly complex (Schaub et al., 2015).

Therefore, it seems desirable to nudge users towards buying more secure devices and taking their privacy into account when purchasing the devices. Governmental bodies could play an active role in reaching this goal, for example by designing legislation or standards that describe which security and privacy related information should be communicated towards consumers and how such information should be communicated.

However, undertaking such initiatives requires detailed and deep insights into the decision-making process of consumers when purchasing IoT devices. More specifically, it is crucial to know how, and to what extent, privacy and security influence the choice of consumers to buy IoT devices. Moreover, the sensitivity of these effects with regard to personal factors should be investigated to evaluate whether the effect of privacy and security differs between various subgroups of consumers. Finally, framing can play a role in the decision-making process. To illustrate this, consumers might take security and privacy into account more strongly when receiving gain-focused security or privacy information (rather than information focused on losses). For this reason, the sensitivity of the effects of privacy and security to framing should be examined. This study aims to provide these insights by answering the following research question:

> "*How do security and privacy influence the choice of consumers to buy an IoT device? And how sensitive is the effect of security and privacy to framing and personal factors?*"

For this study, we focus on the individual consumer as end user of IoT devices, because of our interest in the role of personal factors. The study takes a mixed methods approach towards answering the research question. The quantitative part of the study focuses on quantifying the effect of privacy and security on consumer choice behaviour by developing and testing a causal model that describes the effects of various explanatory factors on choice behaviour. This goal is reached by constructing choice models from data that is gathered from a stated choice experiment. The qualitative part of the study targets the underlying rationales that determine how privacy and security affect consumer choice behaviour by asking consumers open questions regarding the role of privacy and security in their decision to buy or not to buy an IoT device.

The remainder of this paper is structured as follows. Firstly, the next section provides a brief overview of the existing body of literature regarding the research topic in order to develop a conceptual model that forms the basis of this study. Section 3 describes the methods that have been used to conduct the analysis. In Sections 4 and 5, the results of the analysis are presented. Section 6 consists of the conclusions that answer the main research question of the study. In Sections 7–9, the results of the study are discussed in terms of their implication and limitations and possibilities for further research are introduced.

2. Conceptual model

Currently, the effect of security and privacy on the purchase behaviour of consumers has not been studied extensively. However, studies in the Technology Acceptance Modelling (TAM) field have investigated how consumer perception of security and privacy with regard to innovative technologies influences their acceptance. The basis of this field, commonly known as Technology Acceptance Modelling (TAM) has been formed by Davis (1989), who concluded that there exist clear relationships among ease of use, price, usefulness and acceptance of innovative technologies. Davis defined acceptance as the usage of a technology or system by its end users.

In the following years, IT researchers have extended this model by adding perceived security, risk and trust-related factors and applying it to digital products. For example, Gu et al., (2009) applied the Technology Acceptance Model (TAM) to mobile banking. From this study, the authors concluded that trust, ease of use and the acceptance of mobile banking are closely interrelated. Furthermore, a study by Salisbury et al., (2001) evaluated which factors affect the willingness to engage in web-based shopping. The results of this study showed that Web security perception plays a large role in determining purchase intent. Even more, it has a stronger effect than ease of use and usefulness of technology. The authors defined Web security perception as "the extent to which one believes that the Web is secure for transmitting sensitive information" (Salisbury et al., 2001, p. 3). Their measurement of this concept did not take into account any framing effects. On the contrary, positive and negative frames were used additively to determine the security perception of respondents. In line with this thinking, a study by Crespo et al. (2009) has led to the conclusion that various risk factors such as security strongly limit the acceptance of e-commerce. The researchers framed the risk factors as potential losses, without including the effect of framing on choice behaviour. Generally, the studies in the TAM found that attributes related to the functionality, privacy and security of devices have a positive effect on the attractiveness of a device, while attributes related to price have a negative effect on the attractiveness of a device. Therefore, the following hypotheses can be derived:

- H1: The price of an IoT device negatively influences the probability that the device is purchased.

- H2: The number of functionalities of an IoT device positively influences the probability that the device is purchased.
- H3: The security level of an IoT device positively influences the probability that the device is purchased.

The TAM studies discussed above did not include possible effects of framing. Entman (1993, p.2) defined framing as "the selection of some aspects of a perceived reality and making them more salient in a communicating text, in such a way as to promote a particular problem definition, causal interpretation, moral evaluation, and/or treatment recommendation for the item described". Moreover, according to Entman, frames describe problems, diagnose causes, make moral judgements and select the most suited remedies. Chong and Druckman (2007) provide a more high-level definition of framing, defining the concept as "the process by which people develop a particular conceptualisation of an issue or reorient their thinking about an issue".

Gain/loss framing is one of the most prevalent frames in message framing literature. In the gain frame, the message focuses on the gains the decision-maker can acquire when opting for a certain alternative. On the contrary, the loss frame communicates the possible losses of an outcome. According to Prospect Theory, people tend to be risk-averse when being presented with sure gains and risk-seeking when facing sure losses (Kahneman and Tversky, 1979). This goes against classical utility theory, in which similar outcomes provide the same amount of value to the decision-maker. Kahneman & Tversky developed a different choice model, in which value is attained from gains and losses rather than net outcomes and the probabilities in the utility function are replaced by decision weights.

Researchers in the medical field have applied the concept of gain/loss framing in order to assess the effect of gain/loss framing on the choice of patients to opt for a certain treatment. In these studies, gain/loss framing was applied to the communication of treatment information to patients who face the decision to opt for a certain treatment. Armstrong et al. (2002) presented a group of 451 individuals with treatment information. The individuals were randomly divided into three groups. The first group only received the survival rates of the treatment, while the second group received the mortality rates and the third group received both the mortality rates and the survival rates. Upon receiving the information, the individuals were asked to make the decision whether to opt for preventative surgery. The results suggested that individuals who received the mortality rates were less likely to prefer the surgery. These results are clearly in line with the hypotheses of Prospect Theory, as individuals who are presented with the loss frame are risk-seeking and vice versa.

Many studies following a similar procedure have been published during the years. A study by Detweiler et al. (1999) concluded that beachgoers who received a message which focused on the gains of using sunscreen were more likely to buy and use sunscreen. Similarly, Schneider et al. (2001) concluded that a message describing the benefits of stopping had a stronger effect on the willingness of smokers to stop smoking than a message which contained the negative effects of smoking. Kühberger (1998) conducted a meta-analysis of the early contributions in message framing literature. From a sample set of 136 empirical analyses, Kühberger calculated a set of 230 effect sizes. The results were in line with the original hypothesis of Tversky and Kahneman, as messages in the gain frame generally led to risk-averse behaviour and messages in the loss frame caused more risk-seeking behaviour.

Studies in the message framing literature have concluded that messages which focus on gains are more effective in nudging consumers to take preventive measures to mitigate risks. In this line of thinking, buying a secure product or taking privacy into account can also be seen as a preventive measure to mitigate the risk of cyber threats or privacy infringements. Therefore, it can be expected that messages focusing on the gains of buying more secure devices and taking privacy into account are more effective. This leads to the following hypothesis.

- H4: Messages that focus on the gains of security and privacy are more effective in nudging users to purchase more secure devices and consider privacy when buying IoT devices

Thus, a set of four hypotheses have been developed regarding the effect of privacy and security on the purchase behaviour of consumers. These hypotheses are visualised in the causal model in Fig. 1.

3. Method

To test the hypotheses and investigate underlying motivations, we performed both a quantitative and a qualitative study.

3.1. *Quantitative study: stated choice experiment*

The data for the quantitative study has been collected by means of a stated choice experiment. Stated choice experiments are especially suited to analyse the effect of device attributes, personal factors and framing on choice behaviour. In this experiment, the respondents were presented with various choice sets consisting of two smart thermostats. Smart thermostats have been selected since it can be expected that many respondents have some knowledge about the devices due to their availability on the market and widespread use. The alternatives in the choice set varied with regard to three attributes: Price, Functionality and Security. Privacy was not included as an attribute in order to limit the needed number of choice sets per respondent. In order to resemble real-world pricing, the price attribute varied on four levels: €100, €150, €200, and €250. The functionality attribute was coded additively, which implies that the number of functionalities increases as the value of the functionality attribute increases. The following functionalities were included as part of the attribute levels:

1. Remote control (F1): The user is able to remotely access the device in order to adjust the temperature, scheduling or make use of other functionalities.

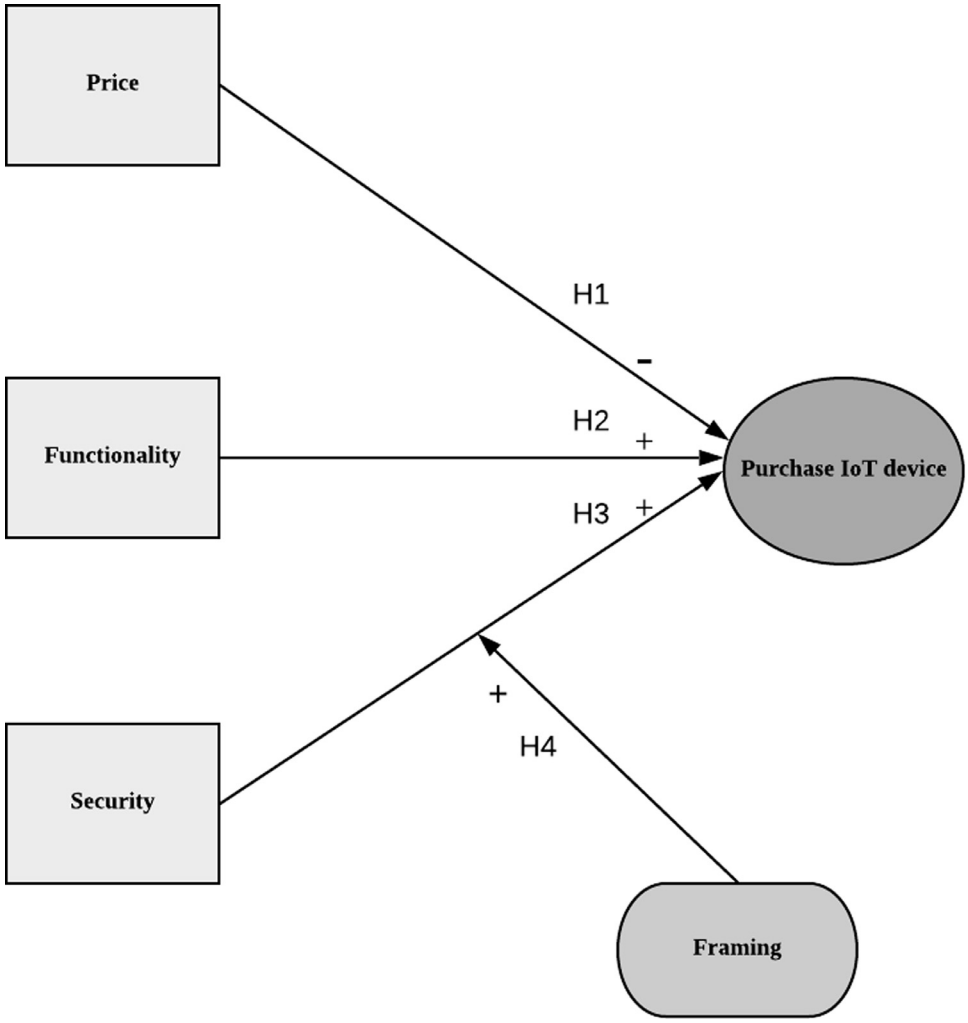

Fig. 1 – Causal model.

2. Geofencing (F2): The geofencing capability of the user's smartphone is used to assess whether the users has left his/her house and adjust temperatures accordingly.
3. Sensing (F3): The home is equipped with sensors, which assess whether the occupants are awake, sleeping or outside of the house. The temperature is adjusted according to the data collected by the sensors.
4. Learning (F4): The user inputs basic schedule parameters. The device makes use of algorithms in order to learn the schedule of the occupants and collects data from sensing to detect changes in the schedule and respond to them.

The security level varied between two levels. Moreover, the respondents in the stated choice experiment were randomly divided into two groups. The descriptions of the security attribute for both levels are displayed in Table 1. For the first group, the security level of the alternatives was framed in terms of gains, while the description of the security level focused on losses for the second group.

With these attribute levels, an orthogonal fractional factorial design was constructed. Each row of the design contains a profile. The choice sets were constructed by means of sequential construction.

Table 1 – Security description.

Frame	Security description
Gain	"This device is/is not secured properly"
Loss	"This device can/cannot be hacked"

Per choice set, the respondents were asked whether they would purchase each individual smart thermostat in the choice set, given that their thermostat had broken and they were faced with the decision to buy a new smart thermostat.

In addition, the respondents were asked questions regarding a set of demographic variables, in order to test the representativity of the collected sample. The following demographics were included in the survey: Age, gender, education level and working situation.

Finally, the survey measured a set of indicators that were expected to play a role in the choice behaviour of consumers purchasing IoT devices. These indicators function as input for a factor analysis, which aims to define a set of personal factors from the indicators. The factors have been constructed by means of Principal Axis Factoring (PAF). This method is

Table 2 – Indicators.

Nr.	Statement
I1	"I keep up with technological developments"
I2:	"I read the technology section when reading newspapers or visiting news websites"
I3:	"I find it interesting to follow the development of new IT products"
I4:	"Innovation is important for economic development"
I5:	"Investments in innovative technologies are important for society"
I6	"If a new IT product has been developed, I want to buy the first version"
I7:	"I pay attention to the security risks of my IT devices"
I8	"When purchasing an IT device, I consider the security risks of the device"
I9:	"The security of my IT devices is important to me"
I10:	"My personal information should be protected sufficiently"
I11:	"I keep track of which information is collected when using online services"
I12:	"I am concerned with the security risks of my IT devices"
I13:	"When using IT devices, I am concerned with the use of my personal data by external parties"
I14:	"When using online services, I am concerned with the use of my personal data by external parties"
I15:	"I undertook action to improve the security of my IT devices"

especially suited to measure the values of non-measurable constructs such as views, opinions and beliefs. The axes have been rotated by means of oblique rotation, which allows for correlation between factors and simplifies the interpretation of factors.

In order to measure the values on the indicators, the respondents were asked to evaluate whether they agreed with a set of statements. The statements are displayed in Table 2.

The survey was spread by a group of BSc students from the faculty of Technology, Policy and Management of Delft University of Technology as part of a data analytics course. The students were asked to share the survey within their social network and collect 5 responses to the survey per person.

3.2. *Quantitative study: discrete choice modelling*

From the collected data, Random Utility Maximisation (RUM) based discrete choice models have been developed. These models describe the probability that a certain decision-maker chooses an alternative from a given set of alternatives which vary on a set of criteria or attributes.

More specifically, Multinomial Logit (MNL) models are used to assess the effects of the attributes, personal factors and framing on choice behaviour. MNL models assume that the error terms in the utility function are independently and identically distributed across all alternatives, which implies that they have the same probability distribution and are mutually independent. The utility of an alternative is calculated by the sum of the product of the criteria scores and a set of linear parameters. Thus, the utility is calculated by the following formula:

$$U(a_i) = \sum_{j=1}^{m} w_j * E\left(a_i,\ c_j\right) + \varepsilon \quad (1)$$

Where w_j is the parameter or weight of attribute j, E (a_i,c_j) represents the expected effect of alternative i on attribute j and ε is equal to the error term.

For MNL models, the probability that an alternative is chosen from a set of alternatives is calculated as follows:

$$P(X = a_i) = \frac{e^{U(a_i)}}{\sum_{j=1}^{n} e^{U(a_j)}} \quad (2)$$

Where $P(X = a_i)$ entails the probability that alternative X is chosen from a predefined choice set, $U(a_i)$ is the utility of alternative i and n is equal to the number of alternatives in the choice set.

For the model selection process, various model statistics are calculated that measure the quality of the developed models. Firstly, the Likelihood Ratio Test (LRT) is used to compare the quality of two models. The statistic that relates to this test is calculated as follows:

$$LRS = -2*(LL_A - LL_B) \quad (3)$$

Where LL_x is the Log-Likelihood of model x.

Secondly, the R-squared value is calculated for each model by dividing the variance of the dependent variable that the model is able to explain by the total variance of the dependent variable.

Finally, an iterative modelling process is applied, which implies that more explanatory variables are added to the model in each iteration to assess whether adding more variables to the model significantly improves the goodness of fit. Table 3 provides a description of the models that are developed in each iteration.

3.3. *Qualitative study*

The qualitative study took a different approach by conducting an online survey in which the respondents were asked open questions regarding their decision to purchase or not to purchase a smart thermostat. The link to the survey was spread via various social media and within the social network of the researcher. Firstly, the respondents were asked which factors had influenced their decision to buy or not to buy a smart thermostat. Subsequently, the respondents

Table 3 – Modelling process.

Model Nr.	Description
1.1	MNL: Device attributes
1.2	MNL: Device attributes + interaction factors and framing with security attribute
1.3	MNL: Device attributes + interaction factors and framing with security and functionality attribute
1.4	MNL: Device attributes + interaction factors and framing with security. functionality and price attribute

Table 4 – Scenarios.

Scenario Nr.	Description
1	The smart thermostat collects data about your energy use and keeps track of your location. A criminal gains access to this information to determine the right moment for a burglary.
2	The smart thermostat collects data about your energy use and keeps track of your location. The producer of your thermostat collects this data and may be obligated to share it with external parties, such as insurers or tax authorities.
3	The smart thermostat collects data about your energy use and keeps track of your location. The producer of your thermostat collects this data and shares it with marketing bureaus, which use it to develop personalised advertisements.
4	A criminal gains access to your smart thermostat, allowing him/her to control the heating in your house.
5	A criminal gains access to your home network via your smart thermostat, allowing the criminal to gain access to personal information on the network, such as passwords or browsing data.
6	Your smart thermostat is part of a large network of devices which is being used to execute cyber-attacks on large organisations.

were triggered to contemplate the role of security and privacy in their decision to buy or not to buy a smart thermostat. Furthermore, the respondents were shown a set of security and privacy risks described by means of hypothetical scenarios. The scenarios were constructed based on known attacks / incidents from literature, and described based on the bowtie framework, i.e. in terms of threat, event, and consequences. We tried to cover a large diversity of threats, incidents and consequences, while keeping the number of scenarios limited. An overview of the scenarios is presented in Table 4. The respondents were asked to rate the severity of each scenario and provide a motivation for their rating on a five-point scale. Finally, the respondents were requested to indicate which scenario described the most severe risk in their opinion. The responses have been analysed with a coding approach by identifying common concepts and their interrelations.

4. Results quantitative study

4.1. *Sample*

For the quantitative study, the students collected a dataset containing 709 respondents. A subset of 93 respondents who did not provide an answer to the questions related to the choice experiment were removed from the data set. Moreover, 35 responses were collected from the same IP address within a distinctly small time frame. These responses were removed from the data set as it is unlikely for such a large number of valid responses to be collected within a small time frame from the same IP address. The resulting sample size used for the analysis is 581.

4.2. *Representativity*

In order to test the representativity of the collected sample, the values of the demographical variables in the sample are compared to the values of these demographical variables for the target population of the study. For this purpose, various Chi-Squared tests have been executed. The results show that the age groups 18-24 years and 50-59 years are overrepresented. Secondly, the sample mostly consists of respondents who have a high education level. Finally, the working situation categories “student” and “paid job” are strongly overrepresented in the sample. These overrepresentations can be explained by the data collection process. The BSc students who spread the survey most likely shared the survey with fellow students, housemates, siblings, parents and other mature family members.

The overrepresentations in the sample might cause under- or overestimation of the average values of the variables considered in the analysis but are less likely to affect the relations between factors, attributes, demographics and choice behaviour. In addition, the main aim of this research is to illustrate that certain relations exist. The overrepresentations do not limit the ability of the developed models to reach this goal.

4.3. *Factor analysis*

From the values of the indicators, personal factors have been deduced by means of Principal Axis Factoring. The resulting factor structure is displayed in Table 5.

The first factor is defined by indicators that relate to the attitude of the respondents towards privacy/security issues of IT devices. Thus, this first factor can be labelled as “privacy/security awareness”. The second factor relates to the

Table 5 – Factor loadings.

Nr.	Factor 1	Factor 2	Factor 3
I1	-	-	-
I2		.785	
I3		.733	
I4			-.888
I5			-.830
I6		.536	
I7	-	-	-
I8	.556		
I9	-	-	-
I10	-	-	-
I11	.534		
I12	.755		
I13	.897		
I14	.833		
I15	.407		
CA	.833	.736	.854

CA = Cronbach's Alpha

Table 6 – Model selection.

Nr.	Log likelihood	R^2	LRT (critical value)
1.1	5054.914	0.265	-
1.2	4580.136	0.297	949.556 (9.488)
1.3	4544.435	0.306	71.402 (9.488)
1.4	4541.340	0.307	6.19 (9.488)

respondent's interest in the development of technology as well as their adoption of new technology. Therefore, the second factor can be labelled as "Technology Acceptance". Finally, the third factor is determined by the two indicators that measure the perceived importance of innovation. The two indicators load negatively on the factor, which implies that the indicators measure the pole opposite of this construct. Consequently, this factor can be labelled as "Conservativeness". The indicators that have been removed from the factor analysis are excluded from the analysis completely, since they do not possess a significantly different meaning than the factors.

Since the factors (and associated items) used in this study were specifically tailored to the contents of this study, they were developed in an exploratory manner. It should therefore be noted that (ideally) the factor structure revealed here should be validated in future studies following a confirmatory approach (based on other samples). That being said, the reliability scores for all three factors (presented in the last row of Table 5) were found to be good (Cronbach Alpha's >0.70). In addition, the (exploratory) factor structure was also subjected to a Confirmatory Factor Analysis (AMOS 25 was used for this purpose). The resulting model showed acceptable model fit according to conventionally used fit criteria ($\chi^2 = 206.6$, df = 41; p = 0.000, CFI = 0.926, SRMR = 0.072) (Hu and Bentler, 1999), which supports the convergent and discriminant validity of the factors. Hence, even though the factors are established in an exploratory fashion, there is sufficient evidence that they are reliable and capture distinctive psychological tendencies that may be assumed to influence choice behaviours of consumers purchasing IoT devices.

Table 7 – Model parameters.

Attributes	Parameter	p
Price (*100 euro)	0.656	0.000
Functionality	0.108	0.000
Security	1.041	0.000
Constant	0.771	0.000
Framing interactions		
Framing * Security	0.041	0.000
Framing * Functionality	0.025	0.264
Framing * Price	-0.025	0.315
Factor interactions		
Technology Acceptance * Security	-0.054	0.092
Privacy/Security Awareness * Security	0.162	0.000
Conservativeness * Security	-0.098	0.001
Technology Acceptance * Functionality	0.095	0.000
Privacy/Security Awareness * Functionality	-0.126	0.525
Conservativeness * Functionality	-0.037	0.152
Technology Acceptance * Price	-0.059	0.045
Privacy/Security Awareness * Price	0.022	0.429
Conservativeness * Price	-0.042	0.132

4.4. *Model selection*

During the modelling process, various models have been developed and assessed by means of the model statistics that have been discussed in Section 3. The models and their respective R-Square value and LRT are displayed in Table 6.

According to the LRT values, model 1.3 provides the best fit to the data. However, the LRT value of model 1.4 is relatively close to the critical value and the model contains a notable interaction effect of the price attribute with the technology acceptance factor. For this reason, model 1.4 is used to draw conclusions in the remainder of this paper.

4.5. *Model parameters*

The parameters of the resulting model, model 1.4 from model group 1, are displayed in Table 7. The parameters in the models indicate how strong a certain attribute influences the utility that is provided to a consumer by a smart thermostat and the probability that the smart thermostat is purchased.

Firstly, the model contains the direct effects of the device attributes on the utility of the alternatives. Thus, three respective parameters have been calculated for each of these attributes; Functionality, Price and Security. The model also contains a constant that describes the expected value or utility of a smart thermostat when each of the attributes is set to 0. Each of these effects is statistically and practically significant. In line with the hypotheses, the price attribute has a negative effect on the expected utility of an alternative. The security level and functionality of an alternative have a positive effect on the utility. The effect of security was exceptionally strong when compared to the other device attributes.

To allow a more intuitive interpretation of the parameters, willingness-to-pay measures can be calculated by dividing the parameters related to functionality and security attributes by the price parameter. This indicates that respondents are, on average, willing to pay 16 euro for each additional functionality (e.g. a thermostat that has geofencing in addition

to remote control), and a premium of 159 euro for a secure thermostat compared to a non-secure thermostat, which is a substantial amount given the provided price range in thermostats (100-250 euro).

Turning to the psychological factors, the technology acceptance factor has significant interactions with the three device attributes. Respondents with a high score on this factor are willing to make concessions on security and price in order to buy the newest technology that provides them with innovative functionalities. Similarly, the privacy/security awareness factor positively moderates the effect of security on the purchase behaviour, which implies that respondents who are more aware of security and privacy risks take security more strongly into account when purchasing a device. Finally, the conservativeness factor negatively interacts with the security attributes. This result suggests that security contributes less to the value of a device for respondents who do not value innovation.

With regard to framing, the results show that security has a stronger effect on the purchase decision for respondents who were faced with the gains of buying a secure device. This finding is in line with the hypothesis of Kahneman & Tversky, who postulated that people are more risk averse when faced with possible gains.

5. Results qualitative study

5.1. *Response*

A total of 27 responses were provided to the survey for the qualitative study. In the collected sample, the higher education levels are highly overrepresented.

5.2. *Purchase decision*

Firstly, the respondents were asked to evaluate what factors played a role in their decision to buy or not to buy a smart thermostat. Strikingly, security or privacy were only mentioned twice as a motivation for the purchase decision. For device owners, the reasons to purchase a smart thermostat were mainly focused around the functionalities the device provides, ease of use and energy cost reductions. With regard to the decision to buy a specific smart thermostat, the compatibility with other devices such as the boiler, voice assistants and smart home devices was mentioned frequently.

After being triggered to actively contemplate the role of security and privacy in their purchase decision, many respondents are able to address some high-level privacy and security related concerns regarding smart thermostats.

The results show that the respondents only start thinking about security and privacy concerns when being actively triggered to evaluate such topics. Without being prompted to think about privacy and security, the respondents focused mainly on other device attributes such as functionality and ease of use.

5.3. *Risk awareness*

15 out of the 27 respondents indicated that they were able to mention security and privacy risks of smart thermostats. The respondents mostly gave high level descriptions of security and privacy risks, using common terms such as “hacking” or “data going public”. It seems notable that the risk descriptions of the respondents strongly lack any detail and are not related to realistic threat scenarios.

5.4. *Scenario’s*

The assessment of scenarios allows for the generation of insights regarding the risk assessment of the respondents. The main goal of the analysis is to determine the underlying factors that influence this process rather than quantifying the effects of these factors. For this reason, the focus lies on analysing the motivations that the respondents have provided for their rating rather than quantitatively assessing the ratings per scenario.

Firstly, the perception of the level of security or privacy related to the device is often mentioned as a motivation to rate a scenario. Some respondents rate the severity of a risk scenario as “low” because they expect that sufficient controls have been put in place. For example, respondents rated the severity of risks in privacy-related scenarios as “low” because GDPR has been put in place and this regulation ought to be sufficient protection against privacy infringements. On the contrary, other respondents mentioned that they perceived the level of security and privacy with regard to IoT devices in general to be low.

Secondly, the probability of occurrence seems to play a role in the risk evaluation process of the respondents. Many respondents have rated the severity of a scenario to be low, as they thought that such a risk would be very unlikely to occur in real life. On the other side, probability of occurrence was also mentioned frequently as a motivation to rate the severity of a risk as “high”.

Thirdly, the benefits for the third party are reported as a motivation for the assessment of a risk. If the respondent is of the opinion that the threat actor in the risk scenario is not able to achieve an attractive benefit, the respondent is likely to rate the severity of the risk as “low”.

Finally, the respondents often mention the impact of a risk scenario as a crucial factor. To illustrate this, scenario 5 (criminal accessing personal information) posed the most severe risk for many respondents, as this scenario has a further reaching impact than the other scenarios. In this scenario, the scope of the impact exceeds the information that is collected, stored and used with regard to the use of the smart thermostat.

6. Conclusions

This study has investigated the effect of security and privacy on the IoT device purchase decision of consumers by answering the following research question:

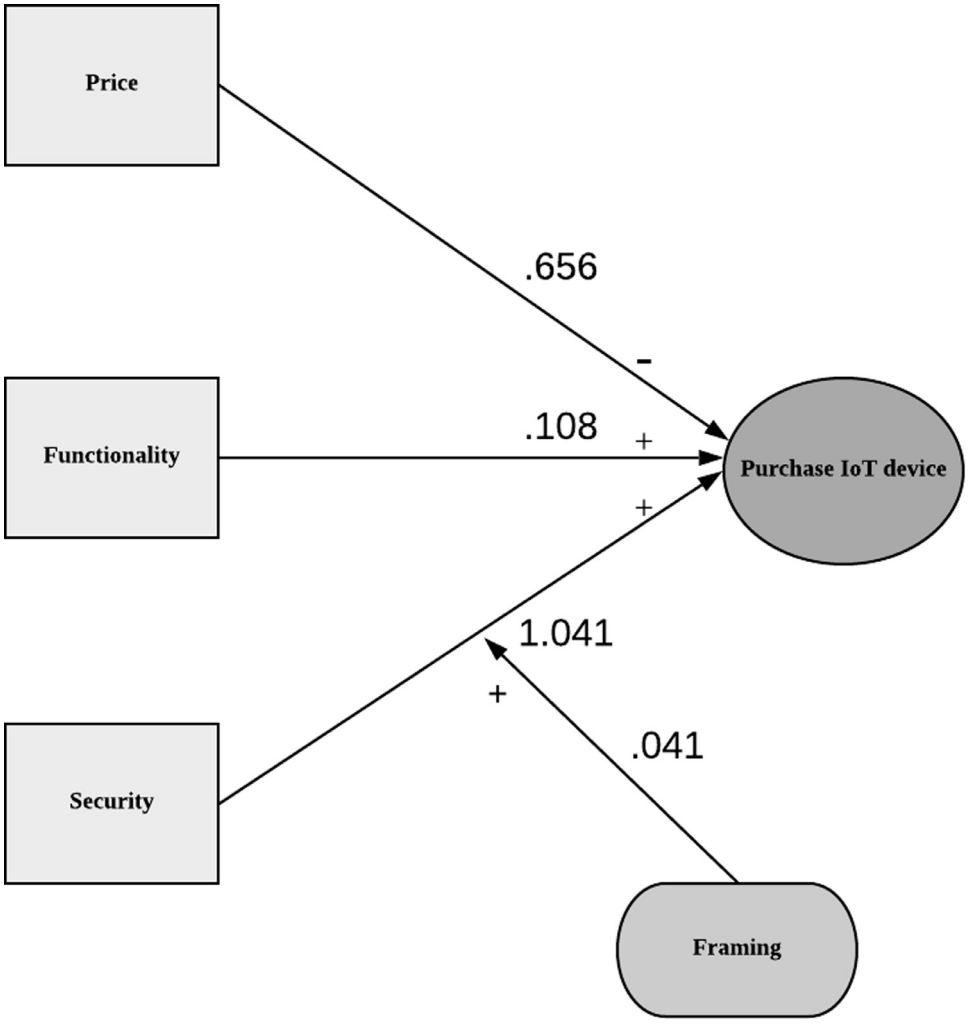

Fig. 2 – Causal model with effect sizes.

"*How do security and privacy influence the choice of consumers to buy an IoT device? And how sensitive is the effect of security and privacy to framing and personal factors?*"

The quantitative part of the study tested a set of four hypotheses regarding the effect of the price, functionality and security of a device on the probability that the device is purchased. The resulting causal model is displayed in Fig. 2.

In line with our hypotheses, the study revealed that security has a notably strong effect on the purchase decision of respondents in a stated choice experiment. On the contrary, security and privacy were only mentioned once or twice as a motivation to buy or not to buy a smart thermostat by the respondents in the survey for the qualitative study. The main difference between both studies is that the respondents in the quantitative study are triggered to think about security, while this is not the case in the qualitative study. Moreover, the respondents in the quantitative study are presented with an easily understandable description of security, which allows them to easily compare alternatives regarding the security level. It is likely that this is not is not the case in real world situations.

The second part of the research question targets the sensitivity of the effect of security and privacy to framing and personal factors. Regarding framing, the results show that security has a stronger effect for respondents who received a gain focused description of security. This finding is in line with the hypothesis of Prospect Theory, which postulates that people are more risk averse when faced with possible gains.

Furthermore, the results have illustrated that consumers who are more aware of the privacy/security risks of (IoT) devices, take security more strongly into account when purchasing IoT devices. The qualitative study also investigated the risk awareness of consumers. The results indicated that some consumers are able to list some of the security and privacy risks of smart thermostats. However, the descriptions of these risks strongly lack detail and are not specific for smart thermostats.

In addition, the qualitative study examined the risk assessment process of consumers. From this analysis, a set of factors have been derived that were frequently mentioned as a motivation to assess the severity of a privacy or security related risk of smart thermostats. The following factors were found to be relevant: Perceived security and privacy level, probability of occurrence, third party benefits, and impact.

Finally, the quantitative study found a negative interaction effect of the technology acceptance factor with the price and security attributes and a positive interaction effect with the functionality attribute. This suggests that people who score high on this factor can be seen as the "first adopters" of innovative technologies and are more willing to buy less secure and more expensive products that do provide them with new functionalities and improve their quality of life.

To conclude, the study has found that security and privacy can have a strong effect on the purchase decision of consumers, under the specific circumstances that privacy and security related information is presented to consumers and is communicated in an understandable manner that allows for comparison of alternative devices in a simple and timely manner. The effect of security is moderated by the privacy/security awareness, technology acceptance and conservativeness of consumers. Finally, the results show that security related information that focuses on the gains of security is more effective in nudging consumers towards buying more secure devices.

7. Discussion

The results of this study have several practical implications. This research has shown that security does affect the purchase behaviour of consumers under the condition that security or privacy related information is presented to consumers and is communicated in a simple and understandable manner. This result suggests that governmental bodies could nudge users towards buying more secure devices and taking privacy into account by ensuring that such communication takes place, allowing for timely comparison of devices with regard to security and privacy. Governmental bodies could work towards this goal by defining standards or legislation that describe what security- and privacy-related information should be provided to consumers and how this information should be communicated. Due to the immense complexity of the IoT security and privacy topic, it is advised to include market parties, such as manufacturers and retailers, in the development process of such legislation or standards.

Furthermore, the results of the study indicate that consumers who are more aware of privacy and security risks are more likely to consider security and privacy when purchasing IoT devices. Thus, improving the risk awareness of consumers supports the goal of nudging users towards buying more secure devices and taking their privacy into account when purchasing devices. In order to reach this goal, governmental bodies could initiate awareness programs that specifically focus on communicating security and privacy risks of IoT devices to consumers. In some countries, such programs have been initiated by governmental bodies. For example, the Dutch government has launched a security awareness campaign specifically targeted at nudging consumers towards updating software in a timely manner. The results of the qualitative study have identified four potential factors that could form the basis of such efforts: perceived security and privacy, probability of occurrence, third party benefits and impact. Finally, the results suggested that the first adopters of innovative technologies can be identified as a potential focus group for awareness campaigns.

In terms of scientific implications, this study shows that stated choice experiments can be used as a method to estimate framing effects. In current studies, framing effects are often evaluated by presenting research subjects with a single choice task. By means of stated choice experiments, the standard errors of the resulting parameters are lowered, thus improving the validity of the developed models. Additionally, the method allows researchers to compare the effects of various attributes on choice behaviour.

In addition, the study contributes to the TAM field by evaluating the effect of various explanatory factors on the purchase decision of consumers. The study differs from the studies in the TAM field with regard to the dependent variable in its causal model. The dependent variable in TAM studies is the acceptance of technologies, while the choice for a specific device functions as the dependent variable in this study. The measurement of the dependent variable also differs from existing studies. In this study, a stated choice experiment is used to measure the choices rather than observing the outcome of a single choice task.

8. Limitations

The quantitative study has observed stated choices rather than choices in real-world situations. It can be argued that this limits the validity of the developed models, as people might exhibit significantly different choice behaviour in the setting of a stated choice experiment. For example, the effect of security might be lower in the case of real-world purchases due to the limited availability of security related information. This might have led to an overestimation of the effect of security in this study.

In real-world choice situations respondents may (wrongfully) assume that IoT products have built-in security. However, the only way to get a sense of how much people are willing to pay for this is by experimentally varying a security attribute, thereby also triggering respondents to pay attention to it in the first place. It may be speculated that when IoT products become more common, people will also gain experiences with possible security risks and/or actual security breaches, which will likely make consumers sensitive to this attribute in future purchases.

Moreover, the alternatives in the stated choice experiment varied on a small set of three attributes. It can be expected that other device attributes, such as ease of use or compatibility with other devices, also have a strong effect on the purchase behaviour of consumers.

Limitations can also arise from the specific coding of the device attributes. In this case, the operationalisation of the security attribute has its drawbacks. The security attribute has been varied on two levels. It is possible that this coding has led to an overestimation of the effect of security on the choice behaviour, as it seems sensible that most respondents would not purchase a device that "is not secured properly" or "can be hacked".

Fourthly, it is questionable whether security and privacy can be framed as a pure gain. To illustrate this, the security

attribute was framed as "this device is/is not secured properly". The term "secured" still suggests that there exists some external threat. This external threat can be seen as potential loss. However, the term "securing" seems a more positive term than "hacking" from a semantic point of view.

MNL models have been developed to assess the effect of security on choice behaviour in the quantitative study. MNL models assume that the error terms in the utility function are independent and identically distributed (i.i.d.). If this assumption is incorrect, this can result in biased parameter estimates.

For the qualitative study, a survey was used to reveal the underlying rationales that determine how security affects the choice behaviour of consumers. A survey allows for the generation of responses in a timely and costless manner. However, using a survey for this goal has its limitations. When using a survey, the researcher is not able to ask follow up questions when needed. An interactive survey design was applied that asked the respondents for more in-depth answers in order to deal with this limitation. Also, because of the overrepresentation of higher education levels, the results of the qualitative study cannot be generalised to the population at large. However, the results still provide insight in possible mechanisms that explain the role of security and privacy in purchase decisions.

9. Further research

In parallel to the study described here, Emami-Naeini et al. (2019) researched how privacy and security factor into IoT device purchase behaviour by conducting a set of 24 semi-structured interviews and spreading a follow up survey to which 200 participants provided a response. The respondents were asked to *rank* certain factors they would take into consideration when purchasing IoT devices. Security was ranked the as the third most important factor, after price and features. By contrast, purchase choices for devices that vary on these attributes are observed in the present study, with the importance of the features derived from the choice models. This confirms that different approaches yield different information regarding purchase behaviour and associated preferences, which we also saw in the differences between our quantitative and qualitative study.

More research is needed to further address the identified knowledge gaps. Firstly, this study only investigated the effect of a limited set of three device attributes. Privacy was not included as a device attribute in this study. In order to assess whether similar conclusions hold for privacy and compare the effects of security and privacy to other device attributes, future research could build upon this study by including privacy and other device attributes.

Secondly, the security attribute was coded as a binary variable, which might have led to the overestimation of the effect of security on the purchase decision of consumers. Future research could evaluate how other operationalisations of security affect choice behaviour in order to determine what operationalisation is most suited to nudge consumers towards buying more secure devices.

Thirdly, this study has observed stated choices rather than real-world choices. Further research could use revealed choice data as an input for the development of choice models to assess whether real-world choice behaviour resembles the choice behaviour in a stated choice experiment. For example, activity on web shops could be monitored to collect data regarding the purchase behaviour of consumers.

Finally, future research could target other stakeholders that buy IoT devices, notably business users. Within this group, a distinction can be made between small companies, which typically do not have security specialists, and large companies, where the security department may be involved in the purchase. Therefore, one would expect purchase decisions in small companies to be similar to individual consumers, whereas decisions in large companies may be less sensitive to additional security explanations.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

Nick Ho-Sam-Sooi: Conceptualization, Methodology, Investigation, Writing - original draft. **Wolter Pieters:** Methodology, Supervision, Writing - review & editing. **Maarten Kroesen:** Methodology, Supervision, Writing - review & editing.

REFERENCES

Armstrong K, Schwartz JS, Fitzgerald G, Putt M, Ubel PA. Effect of framing as gain versus loss on understanding and hypothetical treatment choices: survival and mortality curves. Med. Decis. Making 2002;22(1):76–83.

Chong D, Druckman JN. Framing theory. Annu. Rev. Polit. Sci. 2007;10:103–26.

Crespo AH, del Bosque IR, de los Salmones Sánchez MG. The influence of perceived risk on Internet shopping behavior: a multidimensional perspective. J. Risk Res. 2009;12(2):259–77.

Davis FD. Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Q. 1989:319–40.

Detweiler JB, Bedell BT, Salovey P, Pronin E, Rothman AJ. Message framing and sunscreen use: gain-framed messages motivate beach-goers. Health Psychol. 1999;18(2):189.

Emami-Naeini P, Dixon H, Agarwal Y, Cranor LF. Exploring how privacy and security factor into IoT device purchase behavior. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. ACM; 2019. p. 534.

Entman RM. Framing: toward clarification of a fractured paradigm. J. Commun. 1993;43(4):51–8.

Gu JC, Lee SC, Suh YH. Determinants of behavioral intention to mobile banking. Expert Syst. Appl. 2009;36(9):11605–16.

Hu LT, Bentler PM. Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. Struct. Eq. Model. 1999;6(1):1–55.

Kahneman D, Tversky A. Prospect theory: an analysis of decision under risk. Econometrica 1979;47(2):363–91.

Kühberger A. The influence of framing on risky decisions: A meta-analysis. Organ. Behav. Hum. Decis. Process. 1998;75(1):23–55.

Salisbury WD, Pearson RA, Pearson AW, Miller DW. Perceived security and World Wide Web purchase intention. Ind. Manage. Data Syst. 2001;101(4):165–77.
Schaub F, Balebako R, Durity AL, Cranor LF. A design space for effective privacy notices. In: Eleventh Symposium On Usable Privacy and Security (SOUPS 2015); 2015. p. 1–17.
Schneider TR, Salovey P, Pallonen U, Mundorf N, Smith NF, Steward WT. Visual and auditory message framing effects on tobacco smoking 1. J. Appl. Soc. Psychol. 2001;31(4):667–82.
Sicari S, Rizzardi A, Grieco LA, Coen-Porisini A. Security, privacy and trust in Internet of Things: the road ahead. Comput. Netw. 2015;76:146–64.
Singh KJ, Kapoor DS. Create your own internet of things: a survey of IoT platforms. IEEE Consum. Electron. Mag. 2017;6(2):57–68.

Nick Ho-Sam-Sooi holds an MSc degree in Complex Systems Engineering and management with an IT specialization track at the faculty of Technology, Policy and Management from Delft University of Technology. In addition, he followed several cybersecurity-related courses from the cybersecurity specialization that was organized in collaboration with the University of Twente. For his thesis, he researched the effect of privacy and security on IoT device purchase intent. After completing the thesis and obtaining his degree, he is now working in the cybersecurity field as a consultant.

Wolter Pieters is associate professor of cyber risk at Delft University of Technology, Faculty of Technology, Policy and Management. He has MSc degrees in computer science and philosophy of technology. After finishing his PhD thesis on the electronic voting controversy, he was involved in several projects on cybersecurity risk management, while also publishing on cybersecurity ethics and human factors. He organized several international seminars on emerging topics in cybersecurity, and was program co-chair of the New Security Paradigms Workshop in 2018 and 2019. His current research focus is on cybersecure behaviour and cybersecurity communication.

Maarten Kroesen is associate professor in Travel Behaviour Research at the Faculty of Technology Policy and Management. He has a strong track record in developing and testing novel behavioural theories using advanced statistical methods. His application domain is mostly transportation, but he has published in many other domains (ICT, acoustics, psychology, tourism and health).