

Journal Pre-proof

Nudging purchase intention towards more secure domestic IoT: The effect of label features and psychological mechanisms

Michelle Walterscheid, Nicole Huijts, Iris van Sintemaartensdijk



PII: S2451-9588(24)00019-8

DOI: <https://doi.org/10.1016/j.chbr.2024.100386>

Reference: CHBR 100386

To appear in: *Computers in Human Behavior Reports*

Received Date: 18 August 2023

Revised Date: 7 February 2024

Accepted Date: 24 February 2024

Please cite this article as: Walterscheid M., Huijts N. & van Sintemaartensdijk I., Nudging purchase intention towards more secure domestic IoT: The effect of label features and psychological mechanisms, *Computers in Human Behavior Reports* (2024), doi: <https://doi.org/10.1016/j.chbr.2024.100386>.

This is a PDF file of an article that has undergone enhancements after acceptance, such as the addition of a cover page and metadata, and formatting for readability, but it is not yet the definitive version of record. This version will undergo additional copyediting, typesetting and review before it is published in its final form, but we are providing this version to give early visibility of the article. Please note that, during the production process, errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

© 2024 Published by Elsevier Ltd.

**Nudging Purchase Intention towards More Secure Domestic IoT: The effect of Label Features
and Psychological Mechanisms**

Michelle Walterscheid^a, Nicole Huijts^{a*}, Iris van Sintemaartensdijk^a

michwalth@gmail.com, n.m.a.huijts@utwente.nl, i.vansintemaartensdijk@utwente.nl

^a University of Twente, Faculty of Behavioural Management and Social Science, Drienerlolaan 5,
7522 NB Enschede, Netherlands,

* corresponding author

Journal Pre-proof

Nudging Purchase Intention towards More Secure Domestic IoT: The effect of Label Features and Psychological Mechanisms

Abstract

The domestic Internet of Things market is flooded with unsecure devices and yet, the demand rises. This study aimed to find ways for labels to nudge consumers into purchasing safer devices. Two studies were conducted, one with a Dutch student sample (N = 193) and one with a UK population sample (N = 278). Multiple labels were presented to participants to test potential effects of security degree (high vs. low), framing (positive vs. negative) and label type (grade format vs. informative format), in interaction with initial attitude towards smart devices and trust in the label, on purchase intention. Furthermore, we investigated the antecedents of trust in the label. Findings for both studies indicated significant positive effects of high security degree, positive framing, initial attitude and trust in the label on purchase intention. Both studies find that the positive effect of security degree on purchase intention was stronger when initial attitude was higher and when trust in the label was higher. The informative label was both more trusted and more preferred, so therefore recommended to be used. Overall, security information is effective in steering people towards purchasing safer IoT, and higher trust in the label increases the effectiveness of the label.

Keywords: Domestic IoT; Labels; Security

1. Introduction

The domestic Internet of Things (IoT), more commonly known as smart devices, has been gaining popularity in recent times. Domestic IoT are devices linked within a network, usually to deliver a variety of services in the home, such as gathering data on energy consumption or temperature in order to assist decision-making (Bastos et al., 2018). Smart devices can range from practical utilities like thermostats, vacuums, lights, cameras, or speakers to more entertainment-oriented ones like gaming consoles and TVs (Emami-Naeini et al., 2020). However, domestic IoT devices have serious security and privacy issues, as many devices lack standard security features, and are therefore suffering from cyber-attacks (Bastos et al., 2018). One reason for this issue is that consumers tend to not think about potential security and privacy issues and thus do not take that into account when purchasing smart devices (Emami-Naeini et al., 2019). Furthermore, even if consumers look for

information on security and privacy of smart devices, it is not readily provided by manufacturers and often difficult to find. That is why this study seeks to design and test labels that can facilitate the purchase of safer devices.

Researchers have already been examining the possibility of security and privacy labels on smart device packaging, in order to raise the consumers' awareness (Emami-Naeini et al., 2021; Emami-Naeini et al., 2020; Johnson et al., 2020; Shen & Vervier, 2019). On the basis of prototype studies in the domestic IoT area and on labels from other markets already in use (e.g. nutrition and energy labels), insights have been created on how labels can be designed in such a way that consumers pay more direct attention to security issues and incorporate that in their decision-making. Additionally, previous research has provided insights on more subtle measures that may help to nudge customers away from unsafe devices, such as positive versus negative framing. However, comprehensive, systematic insight into how different label features, in interaction with psychological variables, influence consumer decision making is still lacking.

This study focuses specifically on security of smart devices and aims to investigate how the label features security degree (high vs. low), framing (positive vs. negative) and label type (informative vs. grade) in interaction with the psychological factors initial attitude and trust in the label affect purchase intention of a smart device. We test this with two experimental studies using smart speakers as a case. This study is the first to systematically vary the effects of the label features security degree (similar to nutrition value or energy efficiency in other labels), framing and label type, and test their individual and interrelated effect on purchase intention, in interaction with the psychological variables initial attitude (i.e., the attitude people had about domestic IoT at the start of the study, that is, prior to responding to the labels) and trust in the presented labels in two experimental studies.

1.1. Security and Privacy Issues

In general, domestic IoT are not very secure due to issues such as unencrypted communication and weak or insufficient authentication (Bastos et al., 2018). Moreover, information that is sent to and from the devices without proper encryption can be intercepted and subsequently sold (Karale, 2021). Additionally, certain behaviours from users themselves can exacerbate these issues, like not changing default usernames and passwords or using weak ones which can be easily guessed, or brute forced (Jacobsson et al., 2016). For example, the United Kingdom based organisation "Which?" set up their own smart home and recorded up to 12000 hacking attempts in a week with hackers guessing very simple usernames and passwords (Laughlin, 2021).

Regulation of smart home devices worldwide could be improved as well. For example, while Australia has regulatory laws, local experts in domestic IoT find them deficient as they see that smart devices still have security issues, privacy issues and a lack of industry standard (Harkin et al., 2022). Some countries like India also mainly have general privacy or cybersecurity laws that were not designed with domestic IoT in mind, but manufacturers do have to adhere to these laws (Karale, 2021). There are also countries that have not yet established any suitable laws or policies for smart devices, as is the case for parts of Latin America (Karale, 2021). While the EU, UK and the US already have regulations and are working on improving them, establishing and monitoring new standards across a diverse family of devices is challenging, leading to persistent privacy and security vulnerabilities in devices (Brass et al., 2018). Overall, smart devices worldwide are not sufficiently regulated, especially when it comes to the security and privacy of the devices, making users vulnerable.

The consequences of the lack of security ranges in severity for the individual user. Hackers that gain access to the devices can use them for botnets which can then be used for DDoS attacks or bitcoin mining, which often happens without the awareness of the owner. Hackers that have gained access to stored data can also use it for forging data, blackmailing, extortion, or robbery (Jacobsson et al., 2016) which can be harmful to the individual user. For example, some smart device owners have reported their cameras moving on their own or strangers talking and even threatening them through their devices (Rostami et al., 2022).

One reason for insecure devices in peoples' homes is that people do not sufficiently take security and privacy issues into account before their purchase (Emami-Naeini et al., 2019). Some simply do not find protecting their privacy important, but when they do, they often fail to act in a way that would protect themselves against security and privacy risks, which is also referred to as the privacy paradox (Emami-Naeini et al., 2020; Ghiglieri et al., 2017). Identified reasons for a lack of action are amongst others that the benefits of not taking action outweigh the risks or that people are not aware when their security or privacy is at risk in a specific situation (Barth & De Jong, 2017; Gerber et al., 2018). Furthermore, information on security and privacy risks of smart devices is also difficult to find (Emami-Naeini et al., 2019), making it difficult to consider this information in one's decision making. For example, Blythe et al. (2019) found that most smart device manuals in the UK provide little security information and that comparisons between devices is difficult since the amount of information varies per manual. Studies testing for the effect of security awareness messages show that people adjust their decision making about smart devices when receiving a warning, although the effect seems to depend on whether there is a more secure alternative available that has the

same benefits, since people do not want to lose the benefits of the devices (Ghiglieri et al., 2017; Johnson et al., 2020). Furthermore, a warning seems to lose effect after a certain period of time (Aleisa et al., 2020). This suggests that in the presence of safer alternatives with the same benefits, informing and warning people, particularly shortly before their decision making, could be helpful in nudging people towards buying safer devices. One way to do this is by using labels on smart device packaging, informing people on the security features of the smart devices on sale.

1. 2. Labels

Labels are already successfully used in other areas such as for the the energy consumption of electric devices or for nutritional value of food (Rosenblatt et al., 2018; Schuitema et al., 2020). These labels use different formats to present information, such as using grades going from A to E, or using a traffic light system, providing both exact nutrition numbers and indicating healthiness with the colours green, yellow and red (Blythe & Johnson, 2018). Similar to that, labels on IoT devices could offer information about the security status of smart devices, allowing consumers to swiftly scan labels, get a simple understanding on the security and compare them to other devices. These labels could vary from having more symbolic information about the level of security on a sliding scale, such as a score on a scale from A to E, to having more content wise information, such as indicating whether specific security features are present in the device.

Besides information that is directly relevant for the decision making (e.g. the security degree), labels may also use specific nudging techniques, such as framing. Framing the content of information in a positive or negative manner is one framing technique that might affect the uptake of information. Positive or negative framing means, for example in the context of health information, that a message can either focus on the positive side – promoting health – or the negative side – avoiding illness. In the context of security it means focusing on gaining safety and security or on avoiding risk and insecurity.

Several studies have looked into labels in the IoT context and have been developing prototypes (Emami-Naeini et al., 2020; Johnson et al., 2020; Shen & Vervier, 2019). The study by Shen and Vervier (2019) provides insight into which type of information should be included on the label such as the method of authentication, and the presence of passwords or encryption. The study by Emami-Naeini et al. (2019) provides similar insights but also clarifies preferences of consumers of such information. Systematic testing of different seemingly important label features such as the presented security degree, framing, and label

type on domestic IoT purchase decision making has received little attention in research. The same applies to how the effect of these features on the purchase intention depends on psychological characteristics of the receiver of the information, such as their initial attitude towards the smart device or their trust in the label.

1.3. Label Features and Psychological Mechanisms

To ensure that labels have the desired effect of influencing purchase intentions towards safe devices, certain design practices and psychological parameters that could improve or hinder the effectiveness should be tested. Important factors influencing smart device purchase intention seem to be information about the security degree of the device, the way that security information is framed, the initial attitude people have towards smart devices, their trust in the label information itself and lastly, the label type or the manner in which the information is presented.

1.3.1. Security degree

Security degree is the most important piece of information on a label, telling consumers what the level of security is. Bo et al. (2014) investigated what the most important smart home requirements for users are and found that their participants considered high security to be the most important, more so than an easy set up or manageability. The inclusion of the security degree information could thus steer people towards purchasing more secure devices. Johnson et al. (2020) have already shown that participants are willing to spend more money on devices that have labels with security information on it, especially if the given security degree is high, showing that such labels can be appreciated and effective. Additionally, studies on apps (Choe et al., 2013; Kelley et al., 2013) have shown that privacy-related information also leads to less downloads and lower preferences for more privacy-invasive apps. While these latter studies pertain to privacy of the products, the same could apply to security, and could lead to people considering this information when choosing smart devices that have information on the security degree. Moreover, Ho-Sam-Sooi et al. (2021) found that security degree information indeed had a strong effect on the purchase intention of a smart device. Overall, security degree information is likely to nudge purchase intention towards buying secure devices.

1.3.2. Framing

An additional method that helps with influencing individuals' purchase intention is the way the content of the label is framed. Framing is a nudging technique utilizing differences in

presentation of information to unconsciously nudge individuals' decision-making into a more preferred direction (Choe et al., 2013). Although its influence has been found to be small, it can still lead to behavioural change without enforcing any restrictions (Cahenzli et al., 2021). One way to nudge behaviours through frames is done through either positive or negative framing. Positive framing usually involves focusing on gains or lack of losses, while negative framing focuses on losses or lack of gains (Sparks & Ledgerwood, 2017). Positive and negative framing can be done through colours (green vs. red), symbols (thump up vs. thump down) and semantics. A typical example of semantically framing a message would be "The heart operation has a 95% success rate" versus "The heart operation has a 5% failure rate". The first statement is positively framed as it emphasizes the gains of the procedure while the second statement focuses on the potential losses and is thus negatively framed. In the end both statements have the same meaning, but individuals still perceive the positively framed statement more favourably (Sparks & Ledgerwood, 2017). Donovan and Jalleh (1999) similarly find that positive framing for food products results in more positive attribute ratings of these products, as did earlier studies on the same topic (Levin, 1987; Levin & Gaeth, 1988). Positive framing may thus have a positive effect on attitudes and behaviour towards the involved product.

Previous research has suggested that which type of framing is more effective may depend on the context. Several studies in various fields have suggested that negative framing is more effective than positive framing. For example, in the area of food production, negatively framed health warning messages have been found to be more effective than positive ones for nudging dietary self-control behaviours (Rosenblatt et al., 2018). However, a positively framed message about the fat distribution of beef (90% lean) increased a positive attitude towards the lean product more than a negatively framed message (10 % fat) (Donovan & Jalleh, 1999). Also, in the medical field, negative frames have been generally found to be more effective in eliciting preventive behaviours than positive frames (Banks et al., 1990; Block & Keller, 1999; Maheswaran & Meyers-Levy, 1990). One suggested reason for the stronger effect of negative framing is a negativity bias, suggesting that in general, negative information has more weight than positive information (Kanouse, 1984). However, in the digital context, positive framing may be more effective. Positive framing of reviews and gradings was deemed to be more effective to nudge users away from privacy-invasive apps than negatively framed ones (Choe et al., 2013). In the context of IoT labels, a study by Ho-Sam-Sooi et al. (2021) also found that security degree information was more effective in nudging the purchase of safer smart devices when positively framed (using word the

‘secured’) than when negatively framed (using word the ‘hacked’).

1.3.3. Initial attitude

One psychological factor that can both affect purchase intention, and interact with the message valence of the label itself, is the initial attitude towards domestic IoT. In this case, initial attitude reflects opinions or thoughts about domestic IoT prior to being presented with the devices and their security label. Research has shown that initial attitude is a crucial predictor of the willingness to both purchase and own domestic IoT (van Deursen et al., 2021; Klobas et al., 2019). Specifically, the more positive the attitude is, the more likely it is that devices will be purchased.

Furthermore, initial attitude may affect how presented information is processed and is leading to behavioural intention; particularly alignment or misaligned of initial attitude with the valence of the message may be of relevance. When the message valence is incongruent with initial attitude (e.g. the message is negative about the security while people had positive attitude about smart devices before), consumers may experience cognitive dissonance (Festinger, 1947). Cognitive dissonance theory states that individuals become uncomfortable if their attitude does not match up with what they experience (Festinger, 1957). To reduce this discomfort, individuals can either gain congruence by changing their attitude to match their experience or ignore the information and thus avoid dissonance (Gaspar et al., 2015). When the latter occurs, consumers may thus not change their opinion much after receiving the information. The possibility that new information is to some extent ignored, particularly when the valence of the message is not in line with prior attitude, means that prior attitude is a moderator of the effect of message valence on subsequent decision making.

Message valence of a label on smart devices is both present in the form of the security degree being high or low and in the framing being negative or positive. While there is little evidence on the interaction between initial attitude and high or low security degree, several studies have examined the interaction between initial attitude and positive versus negative framing. Indeed, in these studies, the interaction effect differs based on whether initial attitude and framing are congruent with each other or not, which varies between contexts. For example, in the medical field incongruence between prior negative attitudes and a positive framed message reduced negative attitudes (Fridman et al., 2018). Meanwhile, there seems to be a confirmatory bias in research about trust in food additives information, resulting in messages being more trusted if attitudes and framing are congruent (White et al., 2002).

1.3.4. Trust

Trust in the label itself may also be a factor of concern, since it may affect how the

information on the label is processed. Trust in the source of a message has been found to facilitate behavioural change in accordance to that message. Trust in health experts for example facilitated message uptake and follow up behaviour, of taking preventive measures against Covid-19 (Ahluwalia, 2021). Similar to trust in the source of the message, trust in the message itself may facilitate uptake of the message in the IoT context. When the label is not trusted, consumers may not take the information on it very seriously. On the other hand, when the label information is trusted, the information may be more strongly used in consumers' decision making.

Furthermore, trust in the label may also be affected by the design features of the label in combination with the initial attitude consumers have about the product. Research has shown that participants trust negatively framed information (i.e., meat is 15% fat) more than positively framed information (meat is 85% lean) (Keren, 2007), which is in line with the negativity bias theory, arguing that people tend to trust negative information more than positive information (Kanouse, 1984). White et al. (2003) similarly found that negative information about food additives was trusted more than positive information. However, these latter authors further found that this effect could be explained by the compatibility of the message valence with prior attitude, as a positive message was only distrusted by those with negative prior attitude. The authors thus concluded that participants' trust in a message was dependent on the congruency between the message valence and the prior attitude about the topic. Since message valence is both present in the degree of security and in positive versus negative framing it could also mean that when initial attitude is more in line with security degree or framing (e.g. positive attitude with high security or with positive framing), trust in the label is higher.

1.3.5. Label Designs in IoT

It is important to establish how, and what kind of information should be present on the label, to ensure that the label has the desired effect on the individuals' purchase intentions. There are multiple label types that present information in different ways. Two prominent examples are a grade label that grades the product according to a certain assessment scheme, and an informative label that includes content-related information. The informative labels provide an exact description of the security and privacy measures in a plain text or table format. Unfortunately, these labels often use less known technical terms. Therefore, individuals not familiar with these terms, which are often consumers with a low socioeconomic status, tend to have difficulties understanding the labels' contents (Blythe & Johnson 2018). Comparably, a grade label is easier to understand, simply grading the security

degree using colours, letters, stars or bar length. Grade labels also have an additional effect on decision making since the familiarity of well-known colour coding or letter ranking can invoke the affect heuristic leading to quick and easy decision-making based on that familiarity (Blythe & Johnson 2018). A downside of these labels, however, is that they do not give detailed information, which more knowledgeable consumers might be interested in.

When researching the impact of domestic IoT labels, Johnson et al. (2020) received some feedback from the study participants for their grade label. The grade label had been based on the energy efficiency label and not much adapted to fit the IoT context. Following that, some of the participants pointed out that the grading bars increasing in length as the security degree went down (which makes sense for the energy label as it indicates increased energy consumption) could be confusing for the security context since an increasing length would imply more and not less security. This begs the question how adjusting the grade label to a more intuitive design would affect the relative preference for the two labels, and the relative effectiveness of the labels in nudging people towards more safe smart device choice. In the Johnson et al. study, the informative label was most effective at influencing participants' choices towards secure devices and also the most preferred. This would imply that the informative format is the most suitable choice for promoting security. However, with a better design of the grade label, preferences might shift somewhat.

1.4. The current study

The goal of this study is to find label characteristics that nudge purchase intentions for domestic IoT away from insecure devices. Based on the literature review, the following aspects are examined: security degree information (high vs. low), framing of information (negative vs. positive) and label type (grade vs. informative). Furthermore, we include two psychological variables that may affect the processing of this label information: initial attitude and trust in the label. We will examine the effect of these factors in two experimental studies measuring intention to purchase a smart speaker. We formulate the following hypotheses for the study.

H1a, b and c: High security degree, positive framing, and positive initial attitude have a positive effect on purchase intention.

H2a and b: When initial attitude and the valence of the information on the label (i.e., security degree and framing) are aligned, people have more intention to follow up on the information. This means that the positive effects of high security degree and of positive framing on

purchase intention are stronger when people have a more positive initial attitude.

H3a and b: When people have more trust in the label they are more likely to follow the information on it. This means that when people have more trust in the label, the effect of the information of the label, and particularly security degree and framing, on purchase intention will be stronger.

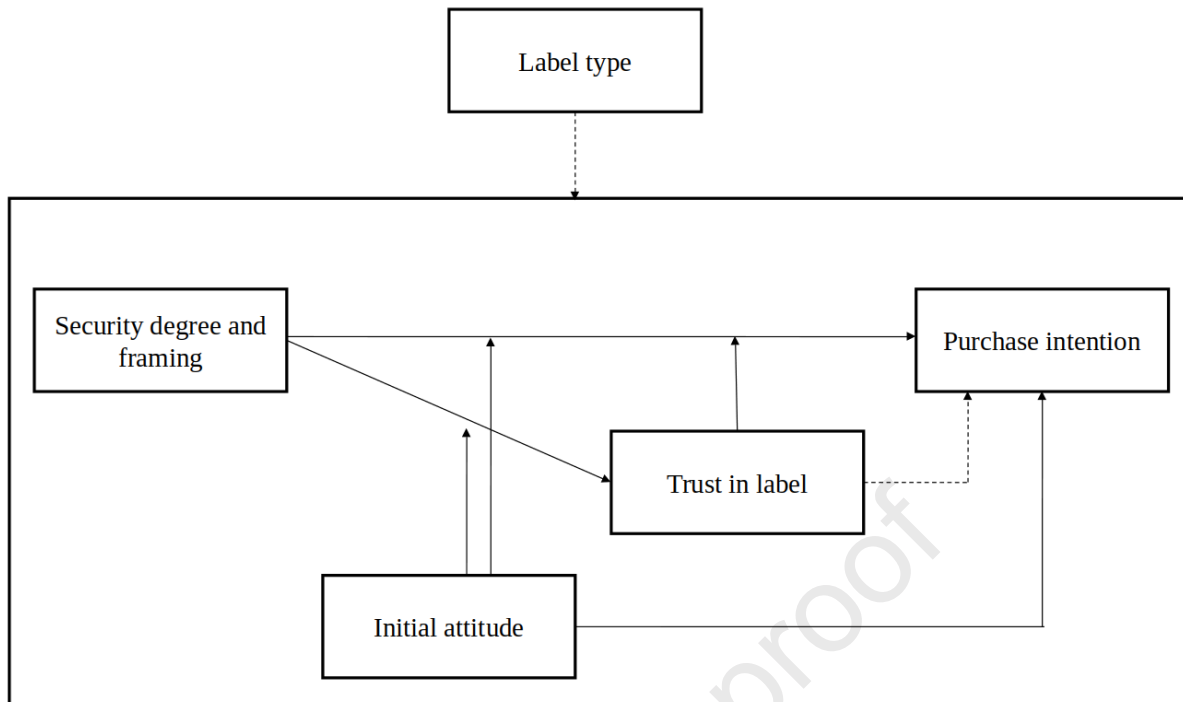
H4a and b: When initial attitude and information on the label (i.e., security degree and framing) are aligned people have more trust in the label. This means that when people have a more positive initial attitude, then high security degree and positive framing will have a more positive effect on trust in the label.

In addition, we explore the moderating effect of framing on the effect of security degree on purchase intention, and the effect of label type on trust in the label and purchase intention and its moderating effect on the effects of security degree, framing, initial attitude and trust in the label.

Finally, we directly elicit the participants' preference for one of the two presented label types and with an open question gauge underlying reasons for this preference as this can further inform the decision making about label formatting. An overview of all hypotheses and explored effects can be found in figure 1.

Figure 1

The conceptual model of the study



Note. The full lines are effects for which there is a directional hypothesis. The dashed lines are effects that are examined/controlled for in the analyses. Note that security degree and framing are two independent variables to which the same hypotheses apply. To improve the readability of the model, these two variables are therefore placed in the same box. Note also that we explore the direct and moderating effect of label type on all dependent variables and on all effects respectively. We additionally explore the moderating effect of framing on the effect of security degree on purchase intention.

2. Study I Methods

2.1. Participants

To gather participants, convenience sampling was utilized by recruiting students from a Dutch university in return for a quarter of a study credit (required to complete their degree), posting links on social media and finally contacting acquaintances working in the educational field. Participants below the age of 16 were excluded from participating in this study. The initial number of recruited participants was 219 but that was subsequently lowered to 193 due to missing values (nine participants had less than 75% completion) and lack of attention (22 did not pass the attention check). The mean age of the participants was 20.5 ($SD = 6.1$). Additionally, 24% were male, 74% were female, and 2% either preferred not to say or chose an alternative option. Most participants were born in Europe and finished high school. See for more detailed information Table 1. Moreover, participants were asked to indicate their

knowledge on smart speakers to get a picture of their familiarity with domestic IoT. Few participants knew nothing at all (3%), while 38% stated they knew a little. Most participants reported to know a moderate amount (47%), while only 8% reported to know a lot and 4% to know a great deal. Lastly, this research project was approved by the ethics committee of the [anonymized] University. See Table 1 for a complete overview of the characteristics of the participants.

Table 1
Profile of participants in study I

	<i>Frequency</i>	<i>Percentage</i>
Gender		
Male	47	24%
Female	143	74%
other	2	1%
Prefer not to say	1	1%
Age		
16-19	83	43%
20-29	109	56%
30 and over	1	1%
Place of birth		
Europe	178	92%
• Germany	102	53%
• Netherlands	53	27%
Asia	12	6%
South America	2	1%
North America	1	1%
Education level		
High school	171	89%
College	8	4%
Trade school	5	2%
Bachelor	8	4%
PhD	1	1%

2.2. Design

The study had a 2 (positive and negative framing) by 2 (informative vs. grade label) by 2 (low vs. high security degree) design, where framing was varied between participants

and label type and security degree were varied within participants. In addition, initial attitude and trust in the label were included as covariates. The independent variables in the analyses were security degree, framing, label type, initial attitude and trust in the label, while the dependent variables in the analyses are purchase intention and trust in the label. An ANOVA was executed to examine if gender, age, education level, and country were randomly distributed across the positive and negative framing group to ensure homogeneity. The variables were not significantly different in both experimental groups suggesting indeed that participants were randomly distributed over the framing groups (See Appendix E).

2.3. Materials

In line with the 2 by 2 by 2 design, eight different labels were designed based on differences in label type, security degree and framing (see Appendix B and C). Label type refers to the differences in presentation of information, being either the grade format (Figure 2) or the informative format (Figure 3). The grade format grades security by differing bar lengths as well as letters going from A to E, combining both the general look of current energy consumption labels used for electronic devices (European Commission, n.d.) and the grading system of food nutrition score labels (Lebensmittelverband, n.d.). Grades were indicated with a black arrow and the higher the grade, the higher the security degree. However, some additional changes were made in order for the energy label to fit into the IoT context. Since participants from the study by Johnson et al. (2020) had indicated that the meaning of a given grade with this kind of label was unclear, it was decided to add a cut-off-line between grading D and C to indicate that a minimum security standard was reached. This indicates that grades above C have the minimum amount of security features to be considered appropriate for this device, while a grade below implied the opposite. This line was captioned with “minimum security standard”. Furthermore, energy labels have bars that increase with length as the grading descends, as that implies greater energy consumption. However, to have increasingly lengthier bars while security decreases can be confusing which is why we designed the security label to have the length of the bars decrease when security features are less present (Johnson et al., 2020 et al.; Choe et al., 2013). Semantic framing was conveyed through the phrasing of the sub-headers on the labels: the positively framed sub-header stated “Protection and security of the device” to emphasize the advantages of security and the negatively framed sub-header stated “Susceptibility and vulnerability of the device” to emphasize the threats of lacking security. Positive framing was further conveyed using the colour green and checkmarks and negative framing using the colour red and alert symbols.

The informative format presented security information in a table and listed the security measures including ‘update’, ‘password’, ‘authentication’, ‘encryption’, ‘internet access’ and ‘connect to other devices’. The table indicated if these security measures are present and, their capabilities (e.g. update: automatic, password: default, updateable). The design and structure of the informative label were inspired by informative labels designed in previous research (Emami-Naeini et al., 2020; Shen & Vervier, 2019), but shortened to mainly include information that is relevant for security. Figure 3 presents the designed label. On the left side of the label, symbols and headings were indicating a security category, with the middle column indicating the exact measures that the category includes. The right column showed if the security measure was present and in case that a certain measure came with different capabilities, the measure was specified. The more features were present, the higher was the security degree, which was additionally indicated through symbols. For negative framing, lacking features were emphasized with the colour red and exclamation points while for positive framing present features were emphasized with checkmarks and the colour green. The semantic framing for the informative label was the same as for the grade label. Additionally, a minimum standard was given through the use of stars; stars next to the features indicate which features were required to pass a minimum security standard, as was also explained in the footnote below the table. This information was thus provided for both label types, to ensure that the two label types convey identical information, other than what we wanted to manipulate.

Figure 2

Grade smart speaker label with high security degree and positive framing

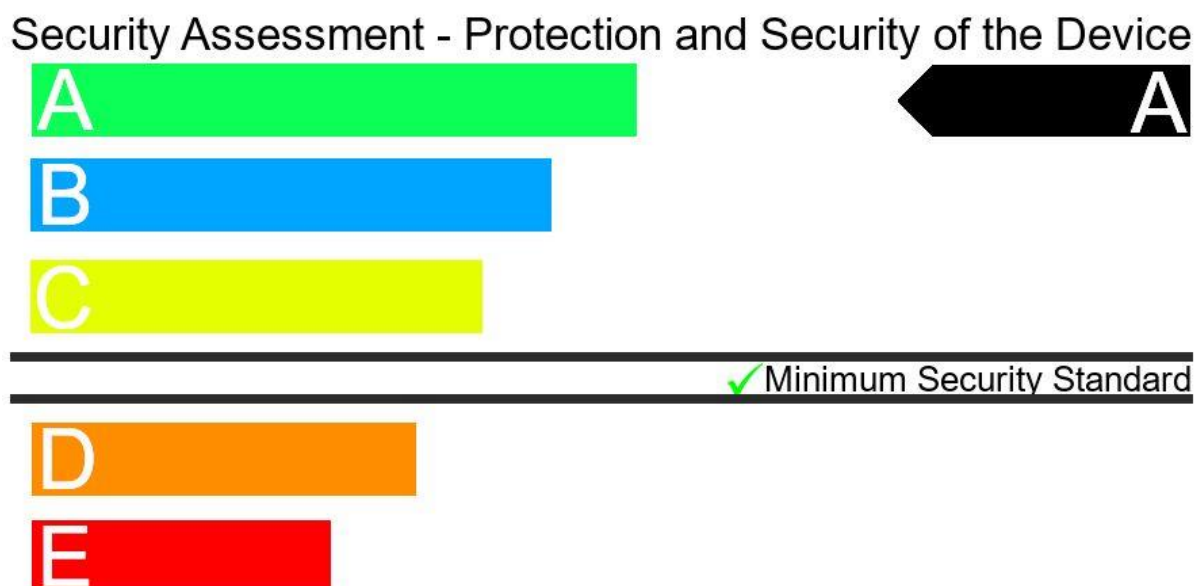



Figure 3*Informative smart speaker label with high security degree and positive framing*

Security Assessment		
Protection and Security of the Device		
Security 	Update*	Automatic ✓
	Password*	Default, updateable ✓
	Authentication*	Two-factor ✓
	Encryption*	Yes ✓
	Internet access	Yes
	Connect to other devices	Yes

* required for minimum security standard

2.4. Measures

2.4.1. Initial Attitude

Initial attitude towards smart devices, while taking security into account, was measured with a slightly adapted scale initially used by Klobas et al. (2019). It is a five item¹, seven-point semantic differential moving from extremely unlikely (1) to extremely likely (7). Participants were presented with the statement “Taking security into account, using a smart home device would be:” followed by adjective pairs like: “Foolish – Wise” or “Worthless – Valuable” (see Appendix A for all items). This was measured at the start of the study to ensure that initial attitude was not influenced by the labels or any other information in the study. Out of the five scales, three were slightly skewed to the left (worthless-valuable, bad idea-good idea, unhelpful-helpful). A factor analysis was conducted to assess if the items measuring initial attitude did not measure multiple different concepts, which was the case (see Appendix D). The item scores were summed up to get an overall attitude score which could potentially range between 5 and 35 points, the middle of the scale being 20 points. The scale was found to be reliable ($\alpha = 0.85$, $M = 20.6$, $SD = 5.98$).

2.4.2. Purchase intention

Purchase intention was measured using one seven point-Likert scale item on the

¹ The measurement originally also included the items Boring-Exciting, but we decided to leave it out as we theoretically did not find it very indicative for evaluating security of a smart home device in a negative or positive sense. This item was therefore also not included in the second study.

likelihood of purchasing the smart speakers running from extremely unlikely (1) to extremely likely (7). The item stated: “How likely are you to purchase the smart speaker based on its description?”, which was asked after each presentation of a smart speaker with a label ($M = 3.30$, $SD = 2.02$).

2.4.3. Trust in the label

Trust in the label itself was measured using one seven point-Likert scale item on the likelihood of purchasing the smart speakers moving from extremely unlikely (1) to extremely likely (7). The item stated: “How likely do you think it is that the description presents correct information” ($M = 4.79$, $SD = 1.46$).

2.5. Procedure

An online survey in English was created using Qualtrics in order to collect data. First, instructions explaining the aims and content of the survey as well as informing the participants that they can quit participation at any point in time were presented. Second, an informed consent form was presented to acquire consent. Participants additionally received the contact information of the researcher to ask questions and to make requests such as the deletion of recorded data. The data itself was anonymous since participants could not be identified as well as confidential since only researchers had access to the data. After that, demographics were collected including: age, gender, country of birth, educational level and initial attitude towards security of smart devices. This was followed by a general explanation of smart devices and their capabilities, so that participants that were not familiar with smart devices could still participate. The participants were presented with a scenario describing that they are looking to buy a smart speaker device, which was followed by the information that smart speakers would be shown to them one after another and the instruction to look carefully at the labels in order to answer the questions following them.

While eight different variations of labels were designed, participants were only presented with four of these labels, due to being randomly grouped in either the positive or the negative framing group. Thus, they were either shown only four positively framed or four negatively framed labels. The first two labels were always graded (see Figure 2), grading the security by colouring, letter and bar length. The last two labels were always informative (see Figure 3), presenting a table listing security features. The order in which label types was presented was not randomized as to not confuse participants with switching the formats back and forth. However, the order of security degree was randomized so that participants could

not anticipate the order of presented labels and determine their answers before looking at them. While being presented with the label, participants were first asked the question that measured purchase intention, followed by the question measuring trust in the label. At the end, participants were shown both label types next to each other and asked to indicate which one they preferred and to add a reason for their preference. Finally, they received a short debriefing of the study goals and were thanked for their participation.

2.6. Analyses

The programs RStudio (version 4.1.2) and Jamovi (version 2.2.5) were used for the statistical analysis of the data. To test the hypotheses, multiple ANCOVAs were executed. For the first hypothesis, an ANCOVA with framing, security degree, initial attitude and trust in the label as predictors and purchase intention as the dependent variable was conducted. For the second and third hypothesis a two-way ANCOVA with the same variables was conducted to specifically assess the interactions of initial attitude with both security degree and framing and the interactions of the variable trust with security degree and framing respectively. In the analyses, all other two-way interactions between all the variables were included to control for and explore other interactions, such as with label type. For the fourth hypothesis another two-way ANCOVA with trust as the dependent variable was created, particularly to examine the interaction of initial attitude with security degree and framing, while controlling for and exploring the direct effects of the variables and other two-way interactions such as with label type. We used simple slope analyses to further examine the significant interaction effects. Additionally, exploratory analyses of three-way interactions were conducted, amongst other reasons to examine for the moderating effect of label type on the hypothesized two-way interactions. Since we did not have hypotheses on the directions of these effects, and since no significant three-way interactions were found, these analyses were moved to Appendix F as a way to reduce the length of the paper. Moreover, we tested if the order in which labels were presented had an effect on results, finding no order effects. To reduce the length of the paper, these results were excluded. Lastly, we summarized the indicated preferences for either the grade label or the informative label, and inductively coded the written responses explaining label preferences.

3. Results

3.1. Purchase intention

In order to test the first hypothesis stating that high security degree, positive framing, and positive initial attitude have a positive effect on purchase intention, an ANCOVA model was created (see Table 2). The analysis additionally explored and controlled for the effect of label type and trust in the label in the analysis.

Table 2

Two-way ANCOVA results for the direct effect of label type, framing, security degree, initial attitude and trust on purchase intention (model 1) and additionally all two-way interactions (model 2)

	<i>F</i>	<i>df</i>	<i>SS</i>	<i>p</i>	η^2
<i>Model 1</i>					
Label Type (grade = 1)	.56	1,763	.93	.455	.001
Framing (positive = 1)	5.27	1,763	8.79	.022	.007
Security degree (high degree = 1)	1007.83	1,763	1681.60	<.001	.571
Initial attitude	75.44	1,763	125.86	<.001	.091
Trust	16.01	1,763	26.71	<.001	.021
R ²	.59				
<i>Model 2</i>					
Label Type (grade = 1)	1.39	1,763	2.20	.239	.002
Framing (positive = 1)	5.93	1,763	9.36	.015	.008
Security degree (high degree = 1)	1051.78	1,763	1661.57	<.001	.584
Initial attitude	61.47	1,763	97.11	<.001	.076
Trust	17.48	1,763	27.61	<.001	.023
Framing*security degree	.02	1,763	.03	.890	.000
Framing*label type	1.05	1,763	1.65	.307	.001
Security degree*label type	.17	1,763	.27	.681	.000
Initial attitude*framing	.01	1,763	.01	.935	.000
Initial attitude*security degree	7.75	1,763	12.24	.006	.010
Initial attitude*label type	3.12	1,763	4.94	.078	.004
Trust*label type	.03	1,763	.06	.850	.000
Trust*framing	2.07	1,763	3.27	.151	.003
Trust*security degree	31.99	1,763	50.54	<.001	.041

Trust*initial attitude	1.21	1,763	1.90	.273	.002
R ²	.61				
ΔR ²	.02				

The analysis showed that there was a significant effect of security degree, framing and initial attitude on purchase intention. Purchase intention was higher for high security degree ($M = 4.77, SD = 1.65$) than for low security degree ($M = 1.83, SD = 1.04$). Purchase intention was also higher for positive framing ($M = 3.43, SD = 2.00$) than for negative framing ($M = 3.19, SD = 2.03$). Further analyses also showed that initial attitude had a positive effect on purchase intention ($B = 0.06, SE = .01, t(748) = 7.84, \beta = 0.18, p < .001$). These results support hypothesis 1a, b and c.

Furthermore, while label type did not affect purchase intention, trust was found to also have a significant effect on purchase intention. Further analyses showed that trust had a positive effect on purchase intention ($B = 0.14, SE = .03, t(748) = 4.18, \beta = 0.10, p < .001$).

The effect of security degree was much larger than the effect of the other four variables, while attitude further has a stronger effect than trust and trust a stronger effect than framing. An overview of mean purchase intention scores per experimental condition can be found in Table 3.

Table 3

Descriptive statistics of purchase intention and trust in the label per experimental condition

	Label Characteristics			Purchase Intention		Trust	
	Security degree	Framing	Label type	<i>M</i>	<i>SD</i>	<i>M</i>	<i>SD</i>
1	high	positive	grade	4.75	1.58	4.09	1.50
2	low	positive	grade	2.01	1.02	4.58	1.51
3	high	positive	informative	5.03	1.55	4.89	1.44
4	low	positive	informative	1.91	1.21	5.03	1.53
5	high	negative	grade	4.68	1.73	4.41	1.43
6	low	negative	grade	1.77	0.94	4.82	1.38
7	high	negative	informative	4.66	1.71	5.21	1.14
8	low	negative	informative	1.66	0.95	5.21	1.45

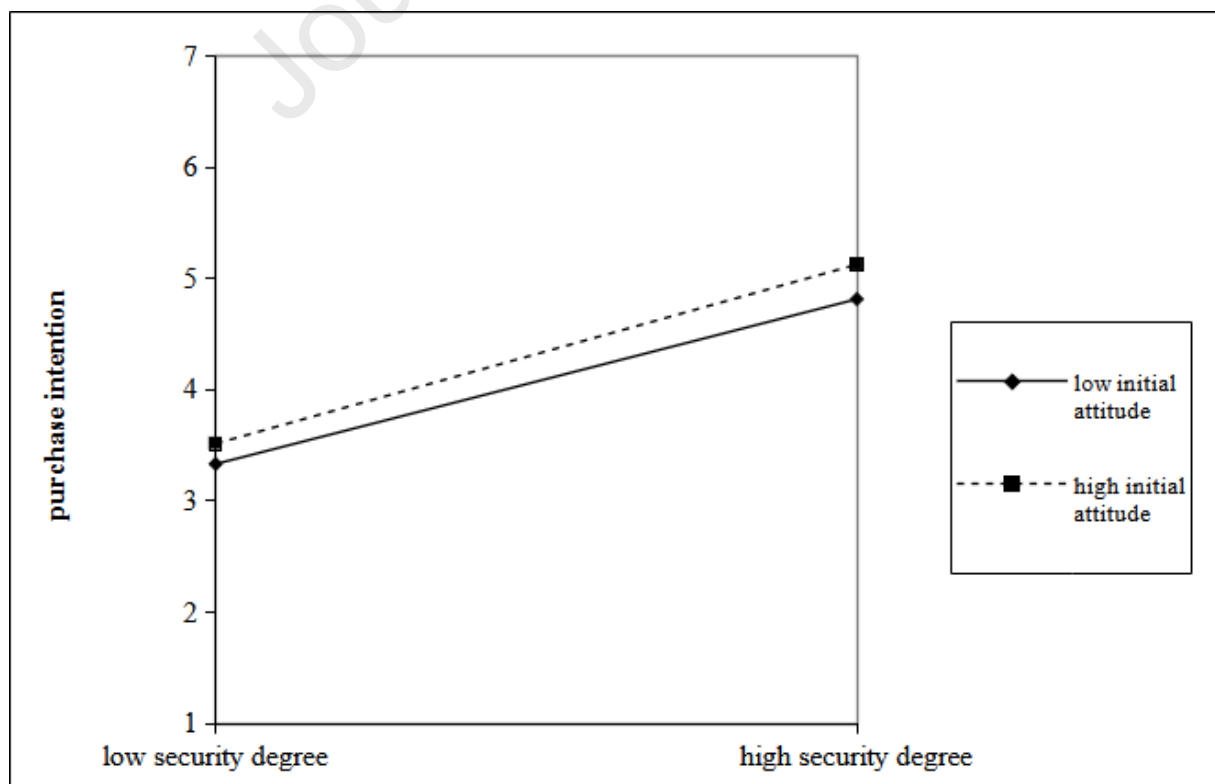
Additionally, to test the second hypothesis that initial attitude moderates the effects of

(a) security degree and (b) framing on purchase intention based on their alignment (in the sense that the positive effect of high security and positive framing on intention is stronger when initial attitude is more positive) and the third hypothesis that when people have more trust in the label they are more likely to follow the information on it (in the sense that when people have more trust in the label, the effect of (a) security degree and (b) framing on purchase intention will be stronger), a second ANCOVA model was conducted. The analysis additionally explores and controls for the other possible two-way interactions such as between framing and security degree, and between various variables and label type (see Table 2).

The findings showed, first, a significant interaction effect between initial attitude and security degree. Simple slope analyses revealed that among participants with low initial attitude (-1 SD below the mean), security degree had a significant positive effect on purchase intention ($B = 2.73, SE = 0.13, t(748) = 20.6, \beta = 1.36, p < .001$), while this positive effect was stronger for participants with a higher initial attitude (1 SD above the mean; $B = 3.25, SE = 0.19, t(748) = 25.2, \beta = 1.61, p < .001$). In line with hypothesis 2a, security degree thus had a stronger positive effect on purchase intention when the initial attitude was higher (see Figure 4). No significant interaction between initial attitude and framing was found, thus providing no support for hypothesis 2b.

Figure 4

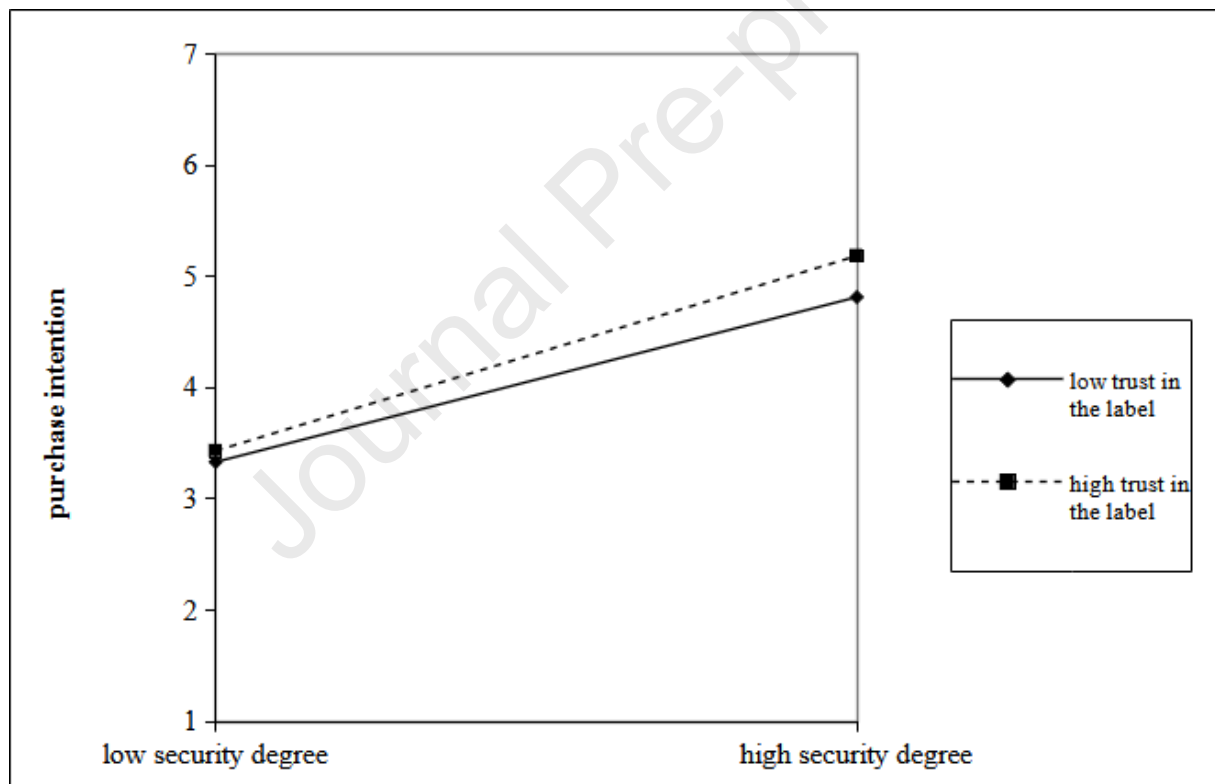
The effect of security degree on purchase intention, moderated by initial attitude



Second, the findings in Table 2 showed a significant interaction effect between trust and security degree on purchase intention. Simple slope analysis revealed that among participants with low trust security degree had a positive effect on purchase intention ($B = 2.45$, $SE = 0.13$, $t(748) = 18.3$, $\beta = 1.21$, $p < .001$), while among participants with high trust this effect was also positive, but stronger ($B = 3.54$, $SE = 0.13$, $t(748) = 26.4$, $\beta = 1.76$, $p < .001$). In line with hypothesis 3a, security degree thus had a stronger positive effect on purchase intention when trust in the label was higher (see Figure 5). We found no significant interaction effect between trust and framing, thus providing no support for hypothesis 3b.

Figure 5

The effect of security degree on purchase intention, moderated by trust in the label



Furthermore, no other significant interaction effects were found, meaning that framing did not moderate the effect of security degree on purchase intention, and label type did not moderate any of the effects of the other variables on purchase intention.

Also in this analysis, security degree was by far the strongest predictor, with initial attitude being the second strongest predictor followed by the interaction between security degree and trust in the label. The interactions between initial attitude and security degree, trust and framing were the weakest predictors. The interactions between security degree and initial

attitude and security degree and trust are relatively small, especially compared to the direct effect of security degree.

3.2. Trust

For exploring the direct effects of label type, framing, security degree and initial attitude on trust an ANCOVA model was created (see Table 4).

Table 4

Two-way ANCOVA results for the direct effect of label type, framing, security degree and initial attitude on trust in the label (model 1) and additionally all two-way interactions (model 2)

	<i>F</i>	<i>df</i>	<i>SS</i>	<i>p</i>	η^2
<i>Model 1</i>					
Label Type (grade = 1)	34.13	1,763	68.0	<.001	.043
Framing (positive = 1)	8.16	1,763	16.3	.004	.011
Security degree (high degree = 1)	6.83	1,763	13.6	.009	.009
Initial attitude	10.28	1,763	20.5	.001	.013
R²	.07				
<i>Model 2</i>					
Label Type (grade = 1)	34.86	1,763	68.26	<.001	.044
Framing (positive = 1)	8.13	1,763	15.92	.004	.011
Security degree (high degree = 1)	7.18	1,763	14.05	.008	.009
Initial attitude	8.54	1,763	16.73	.004	.011
Framing*security degree	.49	1,763	.97	.483	.001
Framing*label type	.12	1,763	.23	.732	.000
Security degree*label type	3.86	1,763	7.56	.050	.005
Initial attitude*framing	4.43	1,763	8.69	.036	.006
Initial attitude*security degree	9.27	1,763	18.15	.002	.012
Initial attitude*label type	1.92	1,763	3.77	.166	.003
R²	0.09				
ΔR^2	0.02				

The results show that label type, framing, security degree and initial attitude

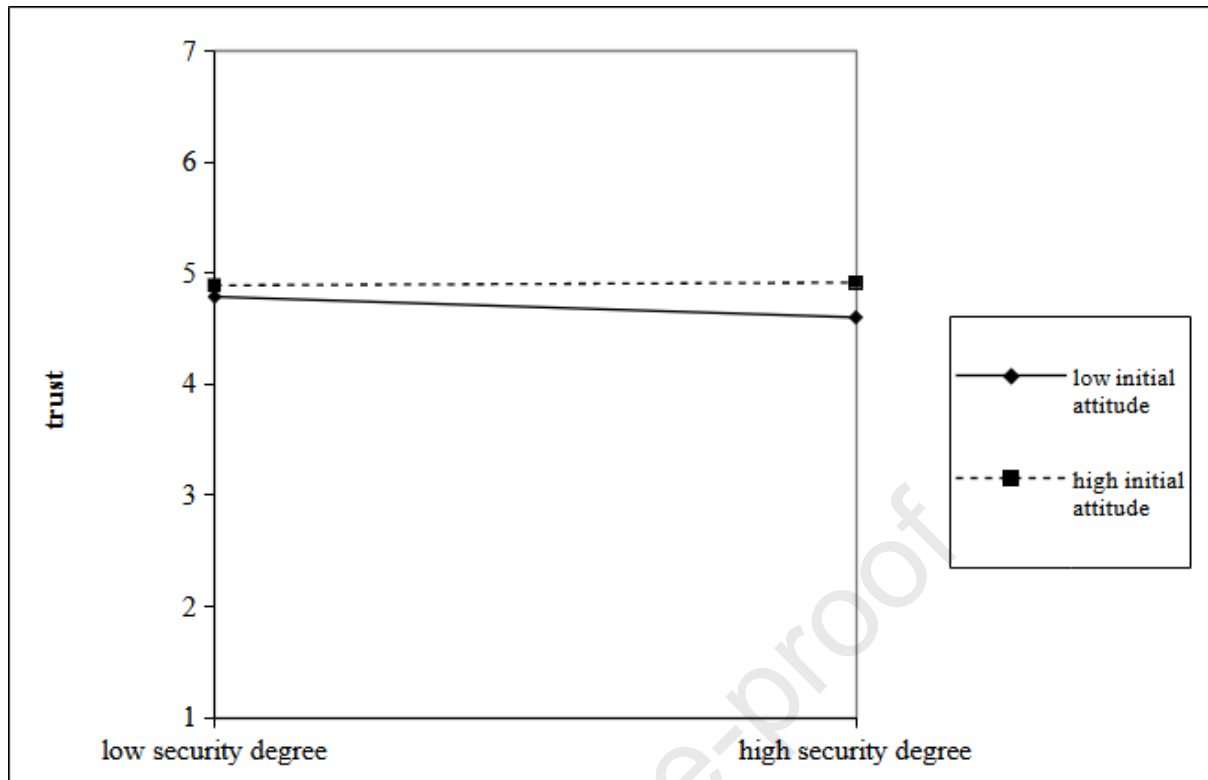
significantly affected trust in the label. Trust was higher for the informative label ($M = 5.09$, $SD = 1.39$) than for the grade label ($M = 4.49$, $SD = 1.47$). Trust was also higher for negative framing ($M = 4.92$, $SD = 1.38$) than for positive framing ($M = 4.65$, $SD = 1.53$), and for low security degree ($M = 4.93$, $SD = 1.47$) than high security degree ($M = 4.66$, $SD = 1.44$). Further analyses also showed that initial attitude had a positive effect on trust ($B = 0.02$, $SE = .01$, $t(759) = 3.21$, $\beta = 0.11$, $p = .001$). The effects were relatively small in size, with label type having the strongest effect, and after that initial attitude, framing and security degree. An overview of mean trust scores per experimental condition can be found in Table 3.

For the fourth hypothesis stating that when initial attitude and security degree and framing align, trust in the label increases, a two-way ANCOVA with trust as the dependent variable was conducted, while other two-way interactions between variables were explored and controlled for (see Table 4).

The results first showed a significant interaction between initial attitude and security degree. Simple slope analysis showed that among participants with lower initial attitude, there was a significant negative effect of security degree on trust in the label ($B = -0.58$, $SE = 0.14$, $t(753) = -4.04$, $\beta = -0.40$, $p < .001$), while among participants with higher initial attitude, there was no significant effect of security degree on trust in the label ($B = 0.03$, $SE = 0.14$, $t(753) = 0.26$, $\beta = 0.03$, $p = .795$). This means that for people who had a lower initial attitude, there was a more negative effect of high security degree, or formulated the other way around, there was a more positive effect of low security degree (which was thus be more in line with their initial attitude) on trust in the label. This provides support for hypothesis 4a (see Figure 6).

Figure 6

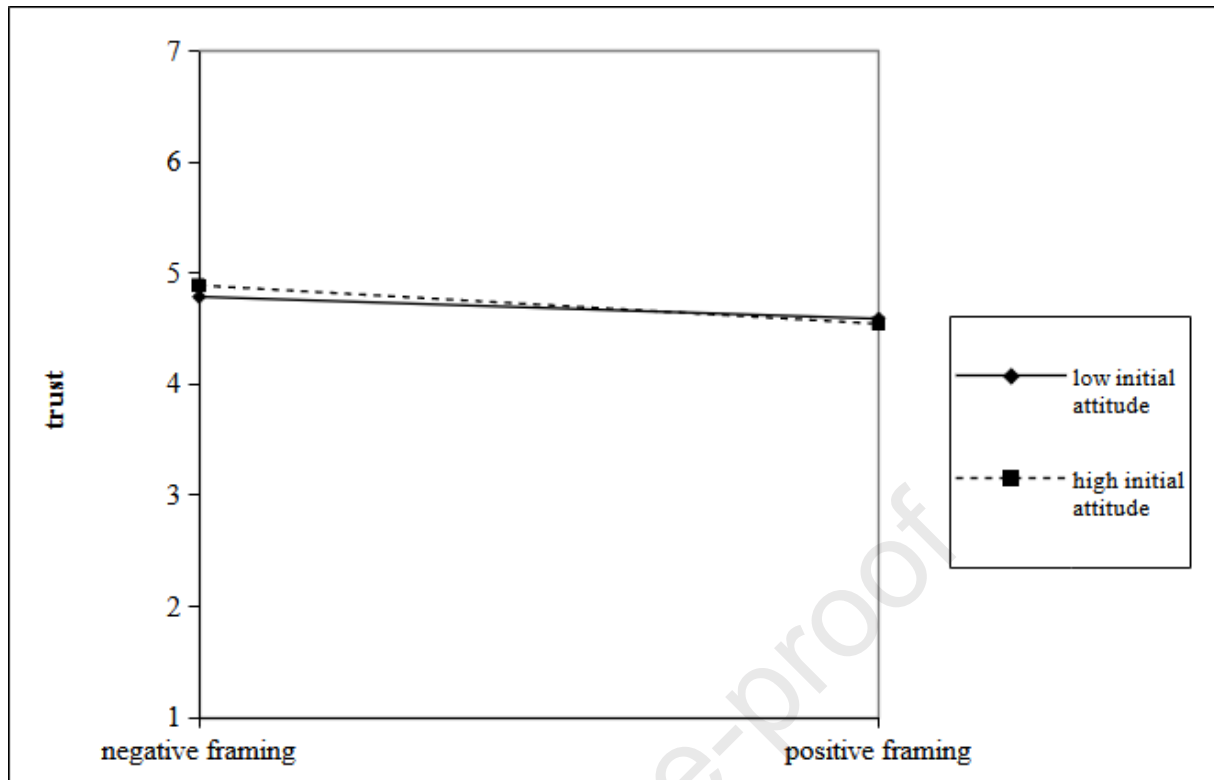
The effect of security degree on trust in the label, moderated by initial attitude



Second, the findings in Table 4 showed a significant interaction effect between initial attitude and framing. Simple slope analysis showed that for people with a lower initial attitude, there was no significant effect of framing on trust in the label ($B = -0.07$, $SE = 0.15$, $t(753) = -0.511$, $\beta = -0.05$, $p = .609$), while for people with higher initial attitude there was a significant negative effect of framing on trust in the label ($B = -0.51$, $SE = 0.14$, $t(753) = -3.53$, $\beta = -0.32$, $p < .001$; see figure 7). This means that positive framing has a more negative effect on trust in the label when initial attitude is higher. This is not providing support for hypothesis 4b, but rather suggesting the opposite effect. No significant interaction effects between framing and security and between label type and other variables were found.

Figure 7

The effect of framing on trust in the label, moderated by initial attitude



3.3. Qualitative research: Label preferences

Participants were asked to indicate their preference for one of the two label types and to add a reason for their preference (which was not obligatory to answer). The responses were inductively coded, resulting in the following codes: ‘easy to understand’, ‘colours’, ‘simplicity’, ‘more information’ and ‘detail’. The findings showed that 74% ($n = 143$) preferred the informative format, while 19% ($n = 37$) preferred the grade format and 6% ($n = 11$) had no preference. Reasons for choosing the informative label were often due to the amount of information ($n = 86$) or detail ($n = 41$) it provided compared to the grade one (e.g. “Gives more detailed information about the features/security details”). Arguments for the grade one were the colouring ($n = 9$) and its simplicity ($n = 5$) (e.g. “Because it has colours and you do not have to read in order to get relevant info.”). However, in both groups a few argued their preferred label type is easier to understand (informative $n = 8$, e.g. “First one is more clear and understandable.”), (grade $n = 14$, e.g. “To me it is more understandable and I like visualizations with colours most.”).

3.4. Summary

In this study, participants were presented with four smart speaker security labels with either positive or negative framing, varying in label type (grade vs. informative) and security degree (low vs. high). The analysis found that positive framing, high security

degree, higher initial attitude and higher trust in the label increased the purchase intention for the smart device. Security degree had the strongest effect and framing the weakest. Initial attitude interacted with security degree but not with framing on purchase intention. Trust in the label interacted with security degree, but not with framing. As expected, security degree had a stronger positive effect on purchase intention when trust in the label was higher. No significant interactions between framing and security degree, and between label type and the other variables were found. Moreover, an informative label, negative framing, low security degree and high initial attitude increased trust in the label, with label type being the strongest factor affecting trust in the label and security degree the weakest. Also, initial attitude interacted with both security degree and framing on trust in the label, but only for security degree, the interaction effect was in the expected direction. Finally, the additional analyses showed that more participants preferred the informative label than the grade label and gave insights into why that was the case.

This study used a convenience sample of mainly students. To have a sample that is more representative of the general population, a second study was conducted with UK participants.

4. Study II Methods

4.1. Participants

Participants were recruited from the Prolific database (www.prolific.co) and received 1.05 pounds for their participation. Participants inclusion criteria included living in the UK, an age range from 18 to 99 years, being fluent in English and having an approval rate between 95 and 100% from earlier studies. The initial number of recruited participants was 305 but that was lowered to 278 solely due to failed attention checks. The mean age of the participants was 38.8 ($SD = 14.0$). Additionally, genders were evenly split and the majority of the participants originated from the United Kingdom (89%; see for more information Table 5). Moreover, participants were asked to indicate their knowledge on smart speakers to get a picture of their familiarity with domestic IoT. About 2% knew nothing at all, 40% knew a little and 39% reported to know a moderate amount. The rest of the participants indicated to either knew a lot (15%), or a great deal (4%). See also Table 5 for an overview of the characteristics of the participants.

Table 5

Profile of participants in study II

	<i>Frequency</i>	<i>Percentage</i>
Gender		
Male	139	50%
Female	139	50%
Age		
18-29	84	30%
30-39	76	27%
40-49	51	18%
50-59	35	13%
60-69	28	10%
70-79	4	2%
Place of birth		
Europe	265	95%
• UK	250	89%
• Other	15	6%
Asia	9	3%
Africa	2	1%
Noth America	2	1%
Education level		
High school	58	21%
College	64	23%
Trade school	10	3%
Bachelor	108	39%
Master	33	12%
PhD	5	2%

4.2. Design

This second study had the same design as the first, a 2 (positive and negative framing) by 2 (informative vs. grade label) by 2 (low vs. high security degree) design. The main difference was that instead of only being shown four labels, all eight labels were presented to each participant. The study included exactly the same variables as the first study, those being security degree, framing, label type, initial attitude, trust in the label and purchase intention.

4.3. Materials

The same eight variations of labels designed for Study I were also used for Study II,

albeit a few adjustments were made based on the results of study I (see Appendix B and C). Specifically, the small effect of framing in study I could have been due to the modest implementation of colouration, while more colours could perhaps grab more attention and lead to a stronger effect. Colour was therefore additionally applied to the arrow on the right side of the label indicating the grade for the grade label; for Study I the arrow pointing out the security degree was black but in this second study it had the same colours as the grade bar (green for high security and red for low security; see for example Figure 8). The changes for the informative label also included adding more colour in order to equalize the amount of colour in both labels. While previously the informative label included a coloured symbol at the end of a row, it is now the rows themselves that are coloured green if framing is positive and red if framing is negative (see for example Figure 9). Similar for the symbols in study I, security degree of the described features determined the amount of rows coloured. In the positive framing condition, if the security degree was high, four of the rows would be coloured green and if the security degree would be low there would be a single green coloured row. Similarly, in the negative framing condition, when security degree was low there were three red coloured rows and no coloured rows if the security degree was high. Additionally, the symbols such as checkmarks and exclamation points remained, but they were no longer coloured according to framing.

Figure 8

New grade smart speaker label with high security degree and positive framing

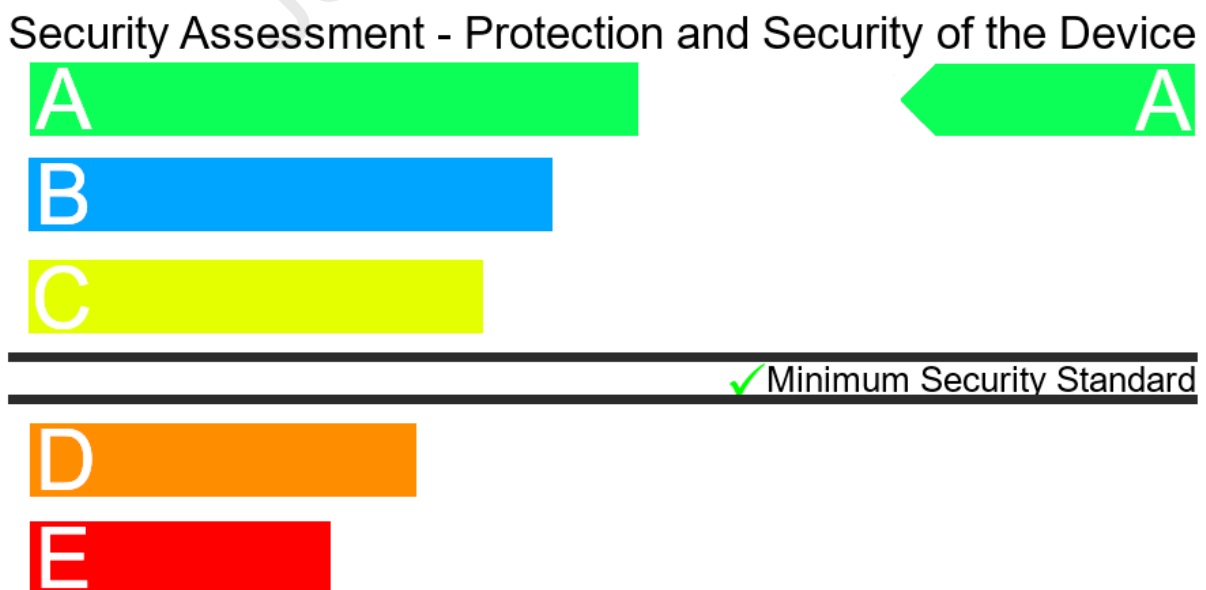



Figure 9

New informative smart speaker label with high security degree and positive framing

Security Assessment		
Protection and Security of the Device		
	Update*	Automatic ✓
	Password*	Default, updateable ✓
	Authentication*	Two-factor ✓
	Encryption*	Yes ✓
	Internet access	Yes
	Connect to other devices	Yes

* required for minimum security standard

4.4. Measures

The measures in this study, being purchase intention ($M = 3.24$, $SD = 2.11$), trust in the label ($M = 5.07$, $SD = 1.57$) and initial attitude, were exactly the same as in study I. For initial attitude, the distributions of the subscales were assessed, revealing all but the Foolish-Wise subscale being skewed to the right. Additionally, factor analysis showed that all items loaded on one factor (see Appendix D). The scale was reliable ($\alpha = 0.94$, $M = 21.0$, $SD = 6.98$).

4.5. Procedure

The previous English online survey created using Qualtrics was adjusted and shared through the prolific website using a link. The initial procedure is identical with the one conducted in study I. However, after the introduction, consent form and collection of demographics, there were differences with the presentation of the labels. To be specific, participants were shown all eight labels instead of only four labels that were randomly either only positively framed or negatively framed. The participants were randomly assigned to either see the four positively or the four negatively framed ones first. Per set of similarly framed labels (positively or negatively), the first two labels that were shown were the grade labels (Figure 8) and the next two labels were informative labels (Figure 9). The order of security degree within the labels was randomized. Another difference with the first study is that while being presented with the label, participants were first asked the question that measured trust, followed by the question measuring purchase intention. The last addition is at the end, when participants were asked whether they preferred a grade label or an informative label, and why, participants in study II could also make suggestions on how to improve or change the labels.

4.6. Analyses

The programs RStudio (version 4.1.2) and Jamovi (version 2.2.5) were used for the analyses. Additionally, the same ANCOVA models from the first study were run. One significant order effect was found for security degree on purchase intention when the framing was positive and label type was informative [$F(2220) = 4.59, SS = 20.33, p = .032$]. In order to control for this order effect a security order variable was added to the analysis². For the open questions inductive coding was used.

5. Results

5.1. Purchase intention

To test the first hypothesis stating that high security degree, positive framing, and positive initial attitude have a positive effect on purchase intention, an ANCOVA model was created (see Table 6). We additionally explored and controlled for the effect of label type, trust in the label and security order (the dummy indicating the order in which security degree was presented) in the analysis.

Table 6

Two-way ANCOVA for the direct effect of label type, framing, security degree, initial attitude and trust on purchase intention (model 1) and additionally all two-way interactions (model 2)

	<i>F</i>	<i>df</i>	<i>SS</i>	<i>p</i>	ηp^2
<i>Model 1</i>					
Label Type (grade = 1)	0.02	1, 2223	0.03	.902	.000
Framing (positive = 1)	22.14	1, 2223	40.84	<.001	.010
Security degree (high degree = 1)	2325.76	1, 2223	4290.48	<.001	.512
Security order (high first = 1)	28.62	1,2223	52.80	<.001	.013
Initial attitude	320.97	1, 2223	592.12	<.001	.126
Trust	181.81	1,2223	335.40	<.001	.076
R ²	.58				
<i>Model 2</i>					
Label Type (grade = 1)	2.42	1, 2223	3.74	.120	.001

² Comparing the analysis not controlling for the order effect to the analysis controlling for the order effect revealed only slight changes in effect sizes either being slightly stronger or slightly weaker.

Framing (positive = 1)	24.92	1, 2223	38.54	<.001	.011
Security degree (high degree = 1)	2642.12	1, 2223	4085.65	<.001	.545
Security order(first high = 1)	26.95	1, 2223	41.57	<.001	.012
Initial attitude	273.45	1, 2223	422.85	<.001	.110
Trust	392.04	1, 2223	508.81	<.001	.130
Framing*security degree	2.18	1, 2223	3.38	.139	.001
Framing*label type	5.55	1, 2223	8.59	.019	.003
Security degree*label type	3.23	1, 2223	5.00	.072	.001
Initial attitude*framing	1.05	1, 2223	1.63	.304	.000
Initial attitude*security degree	23.82	1, 2223	36.84	<.001	.011
Initial attitude*label type	.05	1, 2223	.08	.816	.000
Trust*label type	.98	1, 2223	1.52	.322	.000
Trust*framing	2.30	1, 2223	3.57	.129	.001
Trust*security degree	332.62	1, 2223	514.36	<.001	.131
Trust*initial attitude	1.28	1, 2223	1.98	.258	.001
R ²	.65				
ΔR ²	.07				

For all three variables, significant effects on purchase intention have been found. Purchase intention was higher for high security degree ($M = 4.69$, $SD = 1.82$) than for low security degree ($M = 1.80$, $SD = 1.19$). Purchase intention was also higher for positive framing ($M = 3.39$, $SD = 2.12$) than for negative framing ($M = 3.10$, $SD = 2.09$). Further analysis also showed that initial attitude had a positive effect on purchase intention ($B = 0.06$, $SE = .00$, $t(2203) = 16.51$, $\beta = 0.21$, $p < .001$). The results support hypothesis 1a, b, and c.

Furthermore, while label type did not affect purchase intention, trust in the label and security order were also found to have significant effects. Further analysis showed that trust had a positive effect on purchase intention ($B = 0.34$, $SE = .01$, $t(2203) = 17.88$, $\beta = 0.25$, $p < .001$) and purchase intention was higher for low security appearing first ($M = 3.35$, $SD = 2.11$) than for high security appearing first ($M = 3.16$, $SD = 2.10$), when the label presented was informative and positively framed.

The effect of security degree was much larger than the effect of the other four variables, while initial attitude further had a stronger effect than trust in the label and trust in the label a stronger effect than framing. An overview of mean purchase intention scores per

experimental condition can be found in Table 7.

Table 7

Descriptive statistics of purchase intention and trust in the label per experimental condition

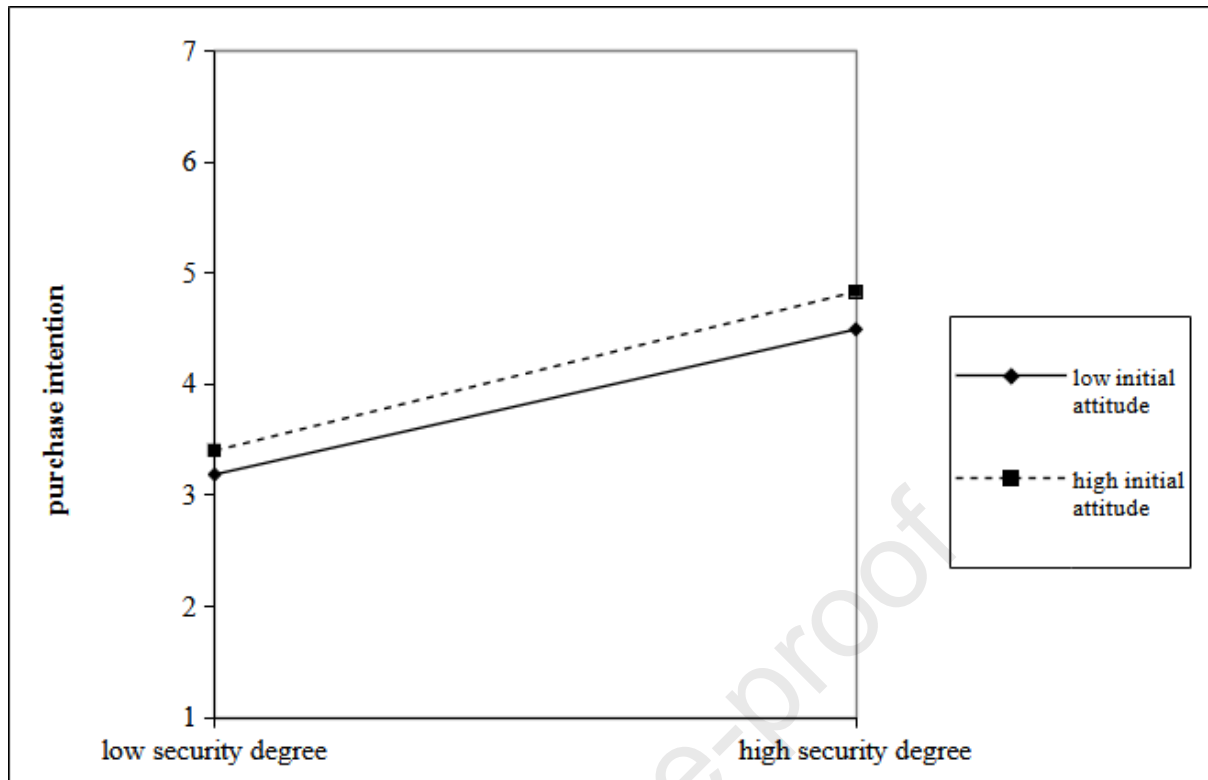
	Label Characteristics			Purchase Intention		Trust	
	Security degree	Framing	Label type	<i>M</i>	<i>SD</i>	<i>M</i>	<i>SD</i>
1	high	positive	grade	4.60	1.85	5.04	1.46
2	low	positive	grade	1.96	1.33	4.88	1.62
3	high	positive	informative	5.02	1.71	5.54	1.16
4	low	positive	informative	1.97	1.28	4.98	1.64
5	high	negative	grade	4.43	1.89	4.98	1.48
6	low	negative	grade	1.83	1.20	4.73	1.81
7	high	negative	informative	4.69	1.76	5.44	1.24
8	low	negative	informative	1.44	.80	4.99	1.84

Furthermore, to test the second hypothesis that initial attitude moderates the effects of (a) security degree and (b) framing on purchase intention based on their alignment and the third hypothesis that when people have more trust in the label they are more likely to follow the information on it, a second ANCOVA model was conducted. The analysis additionally explores and controls for other possible two-way interactions such as between framing and security degree, and between various variables and label type (see Table 6).

The findings showed first, a significant interaction between initial attitude and security degree. Simple slope analysis revealed that among participants with low initial attitude, security degree had a positive effect on purchase intention ($B = 2.49$, $SE = .076$, $t(2207)=33.2$, $\beta = 1.18$, $p < .001$), while this effect was stronger for participants with a high initial attitude ($B = 3.02$, $SE = .077$, $t(2207)=39.2$, $\beta = 1.43$, $p < .001$). In line with hypothesis 2a, security degree thus had a stronger positive effect on purchase intention when the initial attitude was higher (see Figure 10). No significant interaction between initial attitude and framing was found, thus providing no support for hypothesis 2b.

Figure 10

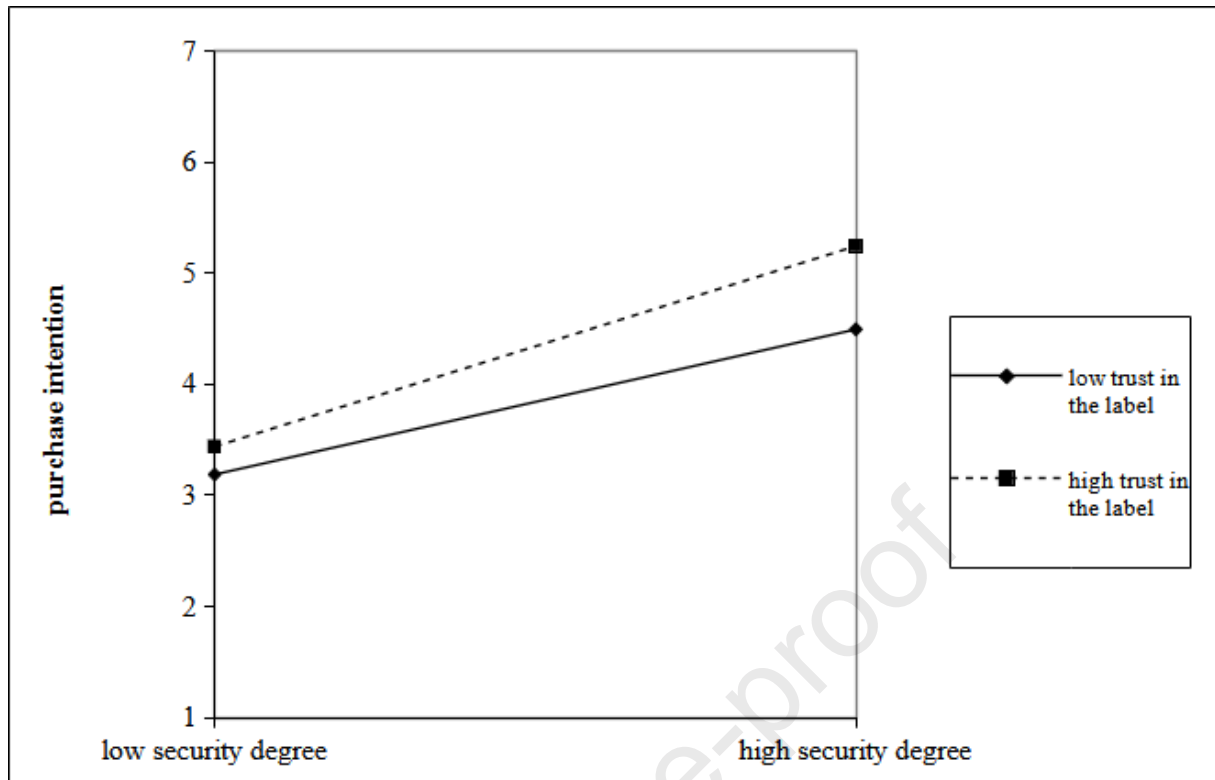
The effect of security degree on purchase intention, moderated by initial attitude



Second, the findings in Table 6 showed a significant interaction effect between trust and security degree on purchase intention. Simple slope analysis revealed that among participants with low trust, security degree had a positive effect on purchase intention ($B = 1.71$, $SE = .08$, $t(2207) = 21.1$, $\beta = 0.81$, $p < .001$), while the effect among participants with high trust was also positive, and stronger ($B = 3.81$, $SE = .08$, $t(2207) = 49.8$, $\beta = 1.80$, $p < .001$). In line with hypothesis 3a, security degree thus had a stronger positive effect on purchase intention when the trust in the label was higher (see Figure 11). We found no significant interaction effect between trust and framing, thus providing no support for hypothesis 3b.

Figure 11

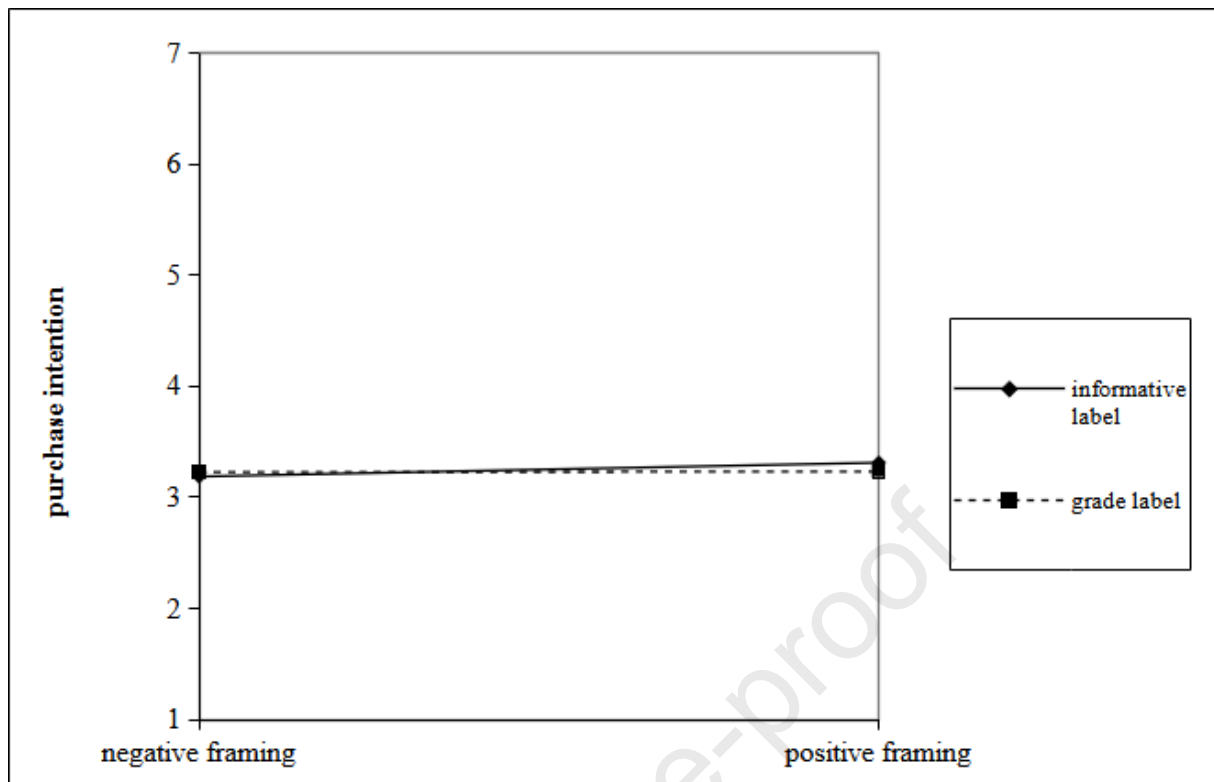
The effect of security degree on purchase intention, moderated by trust in the label



Additionally, the findings in Table 6 showed one other significant interaction effect between framing and label type. Simple slope analysis revealed that when viewing the informative label, there was a significant positive effect of positive framing on purchase intention $B = 0.39$, $SE = .07$, $t(2207) = 5.19$, $\beta = 0.18$, $p < .001$) (see Figure 12). However, for those viewing the grade label, no significant effect of framing on purchase intention was found ($B = 0.14$, $SE = .07$, $t(2207) = 1.85$, $\beta = 0.07$, $p = .065$). Positive framing thus only had a significant positive effect on purchase intention when participants saw an informative label.

Figure 12

The effect of framing on purchase intention, moderated by label type



Furthermore, no other significant interaction effects were found, meaning that framing did not moderate the effect of security degree on purchase intention and label type did not moderate any of the effects of other variables on purchase intention apart from framing.

Also in this analysis, security degree was by far the strongest predictor, with initial attitude being the second strongest predictor, which was followed by the interaction between trust and security degree and the interaction between initial attitude and security degree. Trust in the label, security order, framing and the interaction between framing and label type were the weakest predictors. The interactions between security degree with initial attitude are relatively small, especially compared to the direct effect of security degree. The effect sizes are similar to the previous study except for the effects of initial attitude and trust being somewhat stronger.

5.2. Trust

For exploring the direct effects of label type, framing, security degree, and initial attitude, an ANCOVA model was created (see Table 8).

Table 8

Two-way ANCOVA results for the direct effect of label type, framing, security degree and initial attitude on trust (model 1) and additionally all two-way interactions (model 2)

	<i>F</i>	<i>df</i>	<i>SS</i>	<i>p</i>	η_p^2
<i>Model 1</i>					
Label Type (grade = 1)	25.65	1, 2223	60.6	<.001	.011
Framing (positive = 1)	1.38	1, 2223	3.2	.241	.001
Security degree (high degree = 1)	29.41	1, 2223	69.4	<.001	.013
Initial attitude	43.70	1, 2223	103.2	<.001	.019
R²	.04				
<i>Model 2</i>					
Label Type (grade = 1)	25.98	1, 2223	60.56	<.001	.012
Framing (positive = 1)	1.39	1, 2223	3.25	.241	.001
Security degree (high degree = 1)	29.80	1, 2223	69.45	<.001	.013
Initial attitude	44.27	1, 2223	103.18	<.001	.020
Framing*security degree	.00	1, 2223	.00	.967	.000
Framing*label type	.19	1, 2223	.43	.667	.000
Security degree*label type	5.51	1, 2223	12.84	.019	.002
Initial attitude*framing	.44	1, 2223	1.02	.509	.000
Initial attitude*security degree	25.08	1, 2223	58.45	<.001	.011
Initial attitude*label type	3.74	1, 2223	8.71	.053	.002
R²	.05				
ΔR^2	.01				

The results showed that label type, security degree and initial attitude, but not framing, had a significant effect on trust in the label. Trust was higher for the informative label ($M = 5.24$, $SD = 1.52$) than for the grade label ($M = 4.91$, $SD = 1.60$). Trust was also higher for high security degree ($M = 5.25$, $SD = 1.36$) than for low security degree ($M = 4.89$, $SD = 1.73$). Further analyses also showed that initial attitude had a positive effect on trust ($B = 0.39$, $SE = .07$, $t(2207) = 5.19$, $\beta = 0.1844$, $p < .001$). The effects were relatively small in size, with initial attitude having the strongest effect, and after that security degree and label type. An overview of mean trust scores per experimental condition can be found in Table 7.

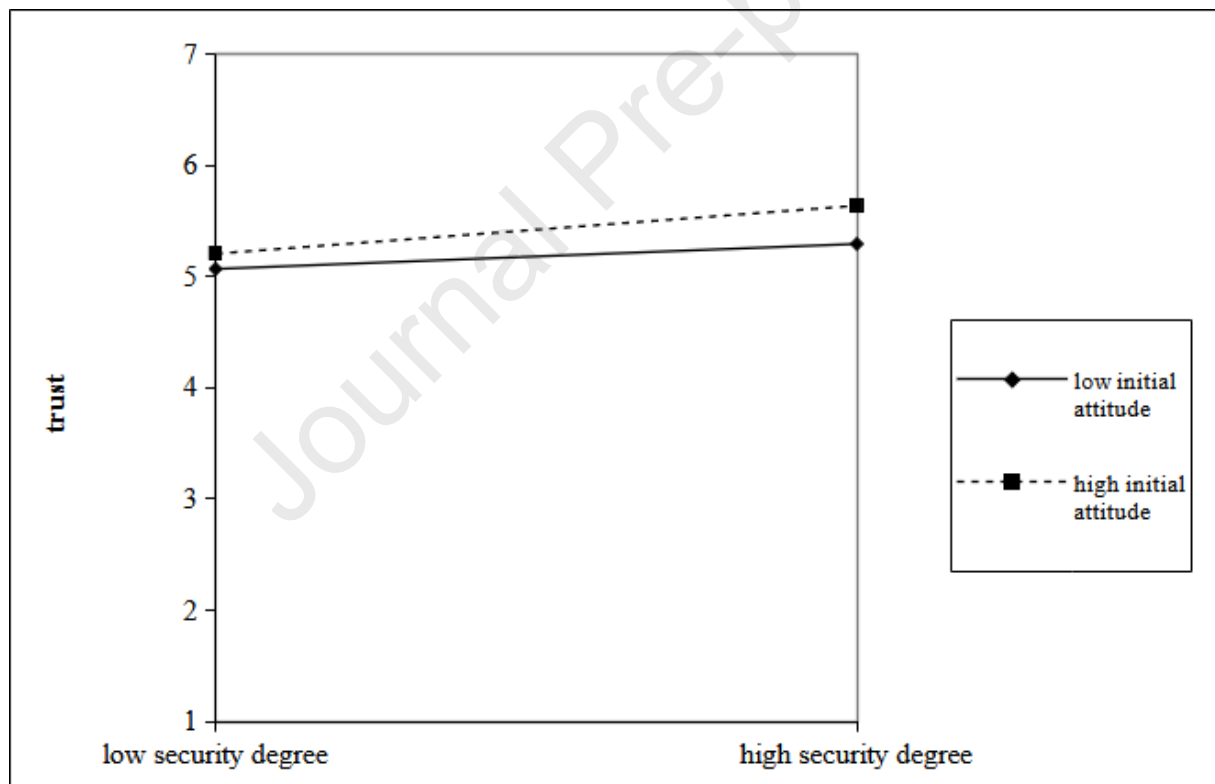
For the fourth hypothesis stating that when initial attitude and information on the label align (i.e., security degree and framing), trust in the label increases, a two-way ANCOVA with trust as the dependent variable was conducted (see Table 8), while exploring and controlling

for other two-way interactions between the predictors.

The results first showed a significant interaction between initial attitude and security degree. Simple slope analysis showed that that among participants with lower initial attitude, there was no significant effect of security degree on trust in the label ($B = 0.03$, $SE = .09$, $t(2213) = .32$, $\beta = 0.02$, $p = .751$), while for participants with higher initial attitude, there was a significant positive effect of security degree on trust in the label ($B = 0.68$, $SE = .09$, $t(2213) = 7.40$, $\beta = 0.43$, $p < .001$). This means that for people with higher initial attitude, a higher security degree (which was thus be more in line with their initial attitude) lead to more trust in the label. This provides support for hypothesis 4a (see Figure 13). No significant interaction between initial attitude and framing was found, thus providing no support for hypothesis 4b.

Figure 13

The effect of security degree on trust in the label, moderated by initial attitude

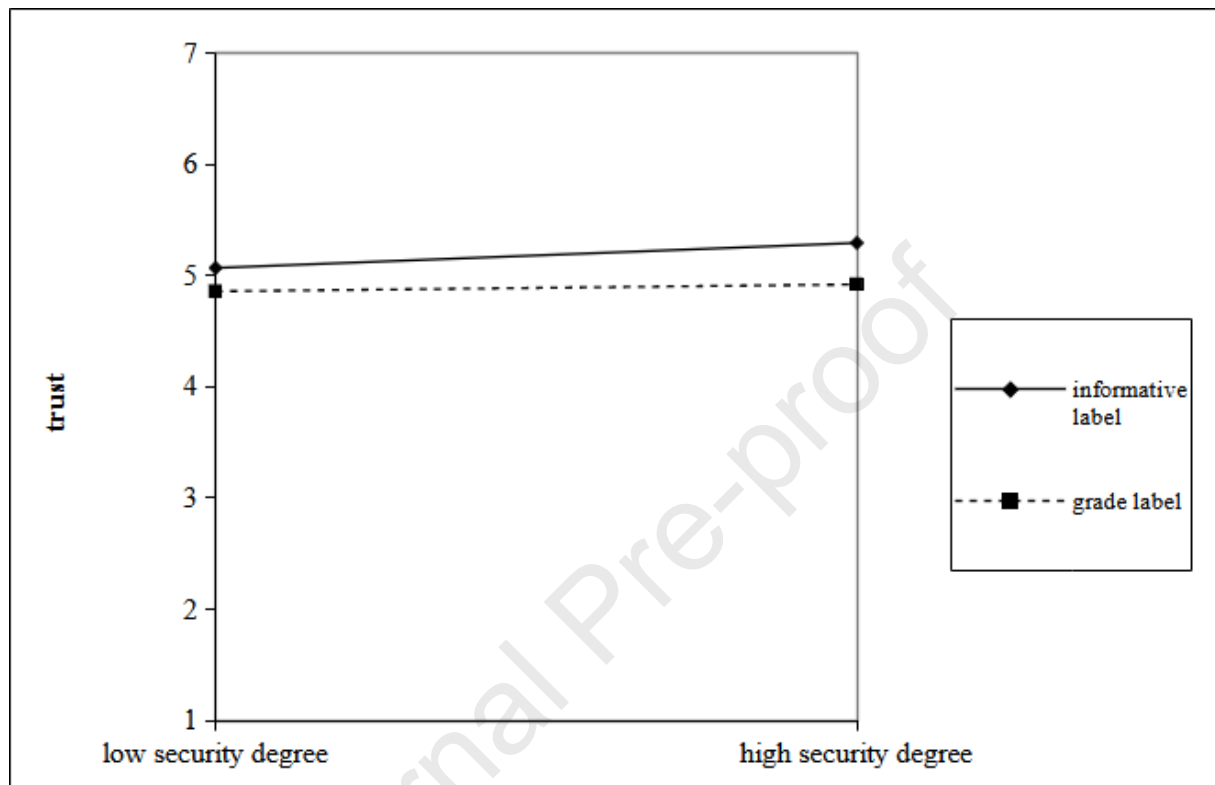


Second, the findings in Table 8 showed a significant interaction between security degree and label type. Simple slope analysis also revealed that for the informative label, security degree had a significant positive effect on trust in the label ($B = 0.51$, $SE = .092$, $t(2213) = 5.52$, $\beta = 0.32$, $p < .001$), while for the grade label, security degree also had a significant positive effect on trust in the label but smaller in size ($B = 0.20$, $SE = .092$, $t(2213) = 2.20$, $\beta = 0.13$, $p = .028$). In other words, the positive effect of security degree on trust in the label was stronger for an informative label than a grade (see figure 14). No significant

interactions between framing and security degree, label type and framing, and label type and initial attitude were found.

Figure 14

The effect of security on trust in the label, moderated by label type



5.3. Qualitative research: Label preferences

Participants were asked to indicate their preference for the label type and could add a reason for their decision as well as add suggestions for improvements or changes in the labels. The responses were inductively coded. Participants tended to prefer the informative label type (77%, $n = 215$) over the grade label type (16%, $n = 45$), while only 7% ($n = 18$) had no preference. The main reasons for preferring the informative label were that it presented more information ($n = 69$) (e.g. "Overall it appears to have more information and I like how the green sections come across as good options"), more detail ($n = 41$) (e.g. "Detailed explanation in regards to particular features providing better overview"), was easy to understand ($n = 24$) (e.g. "The first one makes more sense and is more understandable"), and because it provided more explanation ($n = 10$) (e.g. "It explains much more than just the lines of colour").

The main reasons for preferring the grade type were that it was easy to understand ($n = 10$) (e.g. "It is quick and easy to understand the type of security offered without the need to

read lots of information”), clearer ($n = 6$) (e.g. “it is way easier to read and is eye-catching”) and its visual aspects such as the colours were appealing ($n = 4$) (e.g. “I prefer the colour and visual aspect”). Those not having a preference argued that the two label types presented a trade-off between being either easy to understand but lacking information or being informative but difficult to understand ($n = 3$) (e.g. “Both have merit. The first is good as it gives detail, however the colour and ease of assessing level on the 2nd are more eye catching”). Other reasons were that they do not trust the devices either way ($n = 2$) (e.g. “I do not trust these products, or the information provided to be accurate whatsoever, regardless of the presentation of it”) or that they would never buy smart devices anyway ($n = 2$) (e.g. “I wouldn’t purchase a smart speaker”).

Participants suggestions for improvements and/or changes were either general or pertaining to one of the two labels. A few participants thought it best to combine the two label types ($n = 5$) (e.g. “Maybe a mixture of the two labels with an A-E level of security with A having all the security features etc.”), to add more information ($n = 4$) (e.g. “Give an information leaflet with more information on the list of things stated”) or to explain the minimum security standard ($n = 4$) (e.g. “What the minimum security standard actually is”). For the informative label they also argued to add a letter rating similar to the A-E grading of the grade label ($n = 3$) (e.g. “Maybe have a letter style rating incorporated in the first one”), and to explain things more thoroughly ($n = 2$) (e.g. “More explanation of encryption”). For the grade type they wanted an explanation for the rating criteria ($n = 4$) (e.g. “2nd label could have extra info to what A B C D E F means”).

5.4. Summary

The participants indicated a higher purchase intention when labels had a high security degree and positive framing and when initial attitude and trust in the label were higher. The effect of framing was the weakest and the degree of security was the strongest. Additionally, initial attitude positively interacted with security degree but not with framing. Moreover, a positive significant interaction between trust and security degree on purchase intention was found, but not between trust and framing. As expected, security degree had a stronger positive effect on purchase intention when the trust in the label was higher. There was no interaction effect between framing and security degree. Label type did not affect purchase intention and did not interact with security degree, but did affect the effect of framing on purchase intention. Also, the informative label type, a high security degree and higher initial attitude

increased trust in the label, while framing had no significant effect. Initial attitude had the strongest effect on trust in the label and label type the weakest. Lastly, as expected, security degree had a stronger positive effect on trust in the label when initial attitude was higher and label type positively interacted with the effect of security degree, increasing trust in the label. Finally, the additional analyses on the qualitative data showed that more participants preferred the informative label than the grade label and gave insights into how to improve the labels.

6. General Discussion

The goal of the two studies was to examine the effect of different label characteristics and psychological variables on the intention to purchase a smart device, in order to find insights into how to best nudge consumers towards purchasing safer smart devices. The individual and interrelated effects of label features and individual psychological states have been largely unexplored in the domestic IoT context and thus multiple labels with varying features were created in order to achieve the studies' goal. One such feature was degree of security, with labels presenting a low degree of security or a high degree of security. Another feature was framing the security information either positively or negatively via symbols, semantics and colours. The last feature was label type, presenting either a label with a grade format that graded security from A to E or a label with an informative format with a table that showed which security features were present. We further measured participants' initial attitude on smart devices, and per presented device and accompanying label, we measured intention to purchase the presented smart device, and trust in the information on the presented label. Small adjustments were made to the labels in study II as well as a design change with framing being manipulated within-subject rather than between-subject, but the same manipulations and measures for the variables were used in both studies.

In line with hypothesis 1a, both studies found that high security degree had a significant positive effect on purchase intention. This is in line with earlier research (Johnson et al., 2020) showing that security degree information has a considerable effect on purchase intention. Providing information on the security degree could thus deter consumers from purchasing unsafe devices, instead opting for safer alternatives. Emami-Naeini et al. (2019) found that consumers looking to purchase smart devices considered privacy and security information in their decision, but were troubled by the fact that this information was hard to find. The researchers also added that consumers found this kind of information important and providing it could lead to it being incorporated in the decision-making process to purchase the

devices. The current study thus provides support for this assumption.

Support for hypothesis 1b, stating that positive framing (as compared to negative) has a positive effect on purchase intention, has also been found. This shows that framing by itself affects the purchase intention, independent of whether the information presents a low or high security degree. This is in line with earlier studies on food products showing that positive framing results in more positive attribute ratings of food products (Donovan and Jalleh, 1999; Levin, 1987; Levin & Gaeth, 1988).

Supporting hypothesis 1c, the results show that the initial attitude towards smart devices has a positive effect on purchase intention. This is in line with the theory of planned behaviour, stating that attitudes are a predictor of intentions of behaviour (Ajzen, 1985), and with more recent studies in the IoT context showing that attitudes towards IoT are positively related to the likelihood of acquiring or owning IoT devices (van Deursen et al., 2021; Klobas et al., 2019).

Although we had no a-priori expectation concerning the effect of trust in the label on purchase intention, and thus no a-priori formulated hypothesis, the findings in both studies showed that trust had a significant positive effect on purchase intention. In all experimental conditions, the mean trust level was above the midpoint of the scale, suggesting that participants generally thought that it was to some extent likely that the information on the label was correct. This may mean that the mere presence of the label, when trusted, has a positive effect on purchase intention, which would be in line with the findings that devices that have labels with security information on it (if the given security degree is high) led to a higher willingness to spend money on the device (Johnson et al., 2020).

Also worth mentioning are the differences of the direct effect of security degree on trust in the label between the studies. While for study I, trust in the label was higher for low security degree, for study II trust was higher for high security degree. These opposing findings may possibly be due to the difference in sample demographics between studies. Specifically, study I was composed mainly of young participants, with the majority being female, while the second study had a sample that is more representative of the general population.

We additionally explored a moderating effect of framing on the effect of security degree on purchase intention. Contrary to other studies finding that positive framing increases the effect of a privacy or security message (Choe et al., 2013; Ho-Sam-Sooi et al., 2021) and studies finding that negative framing increase the effect of health related messages (Banks et al., 1990; Block & Keller, 1999; Maheswaran & Meyers-Levy, 1990, Rosenblatt et al., 2018),

no significant interaction effect was found.

In line with hypothesis 2a, both studies found that the positive effect of high security degree on intention to purchase was stronger among people with a more positive initial attitude towards smart devices. In other words, when the security degree on the label was more aligned with initial attitude, people adjusted their intentions more in line with what was on the label. The other way around, when security degree was not aligned with initial attitude, people responded less strongly to the label information. This provides support for cognitive dissonance theory, stating that individuals become uncomfortable if their attitude does not match their experience resulting in incongruence (Festinger, 1947). The response to such discomfort can be either to match their attitude with the experience to gain congruence or to ignore information to avoid dissonance (Gaspar et al. 2015). Particularly the ignoring of the information could explain why people respond less strongly to information when it is not in line with their initial attitude.

Dis-confirming hypothesis 2b, both studies indicated no significant interaction effect between framing and initial attitude towards smart devices on intention to purchase. In other studies that examine the interaction effect between initial attitude and framing, this effect seems context dependent (White et al., 2002; Fridman et al., 2018). Perhaps the context of domestic IoT, unlike the contexts of medical decision making or food industry, is one where this interaction does not occur.

In line with hypothesis 3a, both studies found that the positive effect of high security degree on purchase intention was stronger among people with more trust in the label. Trust in the source of a message has also been found to facilitate uptake and or behavioural change in accordance to that message (Ahluwalia, 2021). The same apparently applies here for the trust in the carrier of the message – the label. While the moderating effect of trust in the label is limited in size and lower trust in the label thus does not very strongly undermine the effect of the label, the effectiveness of the label does increase with stronger trust in the label, making it worthwhile to understand what increases this trust. Both studies showed that the grade label received more trust, indicating that a grade label is better when increasing trust in the label is the main goal.

Dis-confirming hypothesis 3b, both studies found no significant interaction effect between framing and trust in the label on purchase intention. Similarly to hypothesis 2b, the interaction between framing and trust in the label on purchase intention, may simply not apply to the domestic IoT context.

In line with hypothesis 4a, both studies found that the positive effect of high security

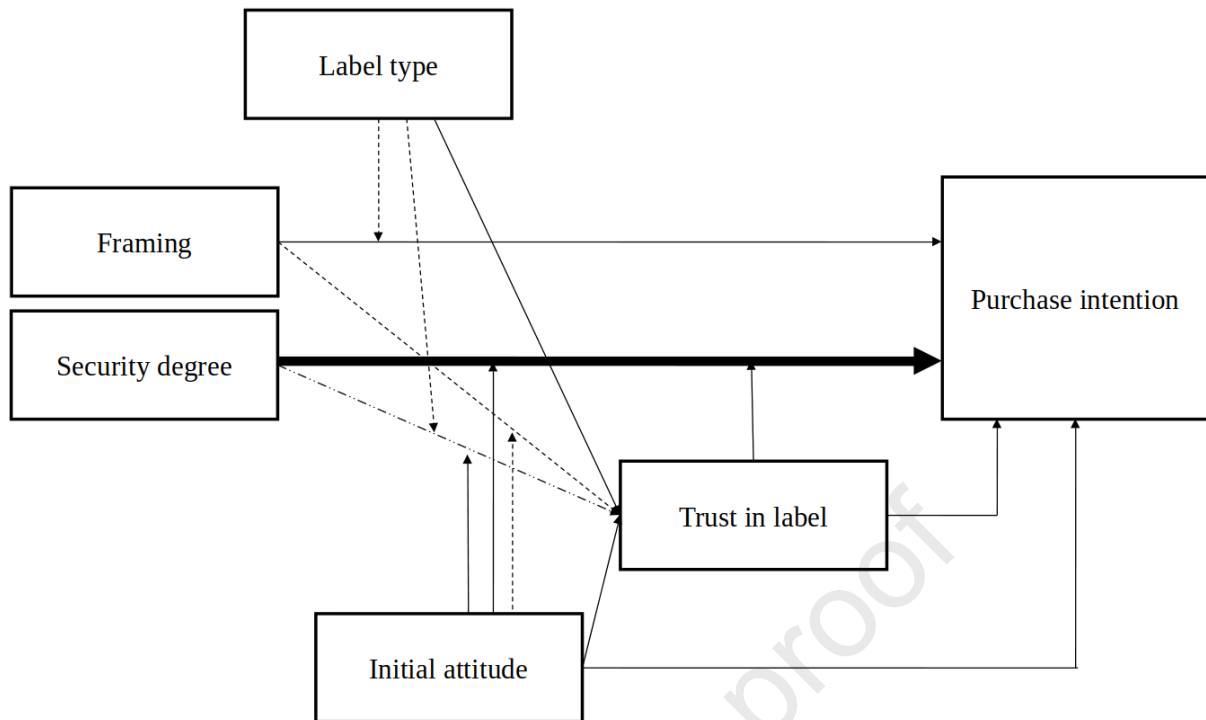
degree on trust in the label was stronger among people with a more positive initial attitude. Furthermore, in study 1, when people with a lower initial attitude saw a label with a lower security degree (which was thus more in line with their initial attitude) they had more trust in the label than when they saw a label with a high security degree. This is in line with White et al (2003), who found that negative information about food additives was trusted more than positive information, and that this effect could be explained by the compatibility of the message valence with prior attitude as a positive message was only distrusted by those with negative prior attitude. In study 1, no effect of security degree on trust in the label was found for people with a more positive attitude. At the same time, however, in study 2 the same interaction effect was found, but here, further analyses showed that while for lower initial attitude, there was no significant effect of security degree on trust in the label, for higher initial attitude there was a significant positive effect of high security degree (which was thus more in line with the initial attitude) on trust in the label. The difference in the mean initial attitude between the two studies was very small and thus not accounting for the differences in the findings between the studies.

Dis-confirming hypothesis 4b, study I found that there is only an effect of framing on trust in the label among people with a higher initial attitude, in which labels with negative framing (thus less in line with the initial attitude) were more trusted than labels with positive framing. This is not in line with White et al. (2003) who found that negative information was more trusted by people with low initial attitude, in other words when message valence and prior attitudes were more aligned. Study 2 did not find support for hypothesis 4b either.

We further explored whether the findings differ between an informative and a grade label. For both studies, label type had no direct effect on purchase intention and hardly any effect on the effect of other variables on purchase intention. One exception is that in the second study label type interacts with framing on purchase intention, finding a positive effect of positive framing on purchase intention when there is an informative label, but not for a grade label. However, in both studies label type did directly affect trust in the label; an informative type resulted in more trust in the label than an informative type. An overview of the findings of the significant effect are in Figure 15.

Figure 15.

A schematic overview of all found effects between variables in study I and II.



Note. The dashed line represents an effect only found in one of the studies. The thicker line represents a relatively strong effect. The double dash and dot line represents an effect that has been found to be significant in both studies but differing in direction.

From the results of the study, a few suggestions for future designs of domestic IoT labels can be formulated that could encourage consumers to purchase smart devices that have a higher security standard. Naturally, the most important information is a form of security rating. Out of the examined factors, security degree was by far the strongest predictor of purchase intention, as consumers are much more willing to purchase devices with a high level of security, compared to devices with a low level of security, independent of the presentation (grade vs. informative label) of that information. The results of this study indicate that a direct security ranking using letters from A to E (i.e., the grade label) works just as well as an implied security rating that simply lists the security features (i.e., the informative label).

Moreover, framing can be implemented on labels through general colouration (red vs. green), symbols (alert icon vs. checkmark) and wording (susceptibility vs. protection). Positive framing leads to a higher purchase intention than negative framing, and may therefore be preferred from an economic point of view, but does not steer consumers towards buying a more secure device specifically. In the second study, the framing manipulation was made slightly stronger by a stronger presence of the colours indicating the security degree. In line with that, the effect of positive framing on intention was also a bit stronger in study II. Further research could further clarify how small differences in the design affects decision

making.

Personal factors such as initial attitude and trust in the label had a stronger effect on purchase intention than framing, but their effect was not as strong as the effect of security degree. Furthermore, while both initial attitude and trust in the label moderated the effect of security degree, that moderation was limited in size, and thus did not strongly affect the effectiveness of the security degree on the label.

While label type did not directly affect the effect of security level on purchase intention, the informative label was found to be more trusted, and higher trust increased the effect of security degree on purchase intention, so it could be argued that indirectly, the informative label did also lead to more secure purchase intentions. In line with a study by Johnson et al. (2020), answers to an additional closed and open question about which label type participants preferred also showed that more participants preferred the informative label type than the grade one. The stated reasons for preferring the informative type was mostly about it providing detailed information. Overall, this suggests that the informative label is both more effective and more preferred. Furthermore, the second study found a moderating effect for label type, as it showed that for the grade label positive framing had a somewhat stronger positive effect on purchase intention than for the informative label.

As many of the participants also expressed interest in more information, it may additionally be helpful to include even more information, for example by presenting further information online. Since a part of the participants nevertheless preferred the grade label, for reasons such as the label's simplicity and having trouble understanding the informative one, and since a few of the participants even suggested that they would prefer a combination of the labels, it seems that a combination of the two label types such as an informative table with both grading using letters or stars and detailed information would be even more ideal. By providing both, consumers can both easily understand and compare devices without requiring prior knowledge, but also get more in-depth information if desired.

6.1. Future research

Considering that, the stated reasons for the preference of either label type seems to have been based on the individual level of knowledge on smart devices, knowledge and understanding of domestic IoT should be included in future research as it may further influence the effectiveness of specific labels. In addition to that, since our recommendations suggest a label combining a grade and informative label, it would be worthwhile to have studies comparing the effects of the grade and informative labels to the effects of a combined

label.

Based on our findings, more trust in the label would increase uptake of the information on the label and thus lower the purchase of unsafe devices. Both studies suggested that an informative label was more trusted. Trust in the label could perhaps, however, also be increased if the security information on it is reported to come from a source that is seen as credible, such as for example from independent experts (Schuitema et al., 2020). This could be shown through multiple ways, such as a product seal or QR-code of assessors. Possibly other design features of the label, such as its shape, letter type, etc. could also affect the trust in the label. Future studies could thus explore which information source is considered most credible, but could also examine which design is the most effective in increasing trust to get a standardized label scheme.

Moreover, it is not known how much attention was given to the different elements in the label. An eye-tracking study could uncover what people pay attention to which could inform further design changes. Adjusting the label accordingly could perhaps make the security information even more noticeable and convincing. For example, Waechter et al (2015) used eye-tracking to analyse the effects of a refrigerator energy label and found that, while the label increased participants focus on energy-related information and energy-efficiency information, energy-related information was not processed unlike the energy-efficiency information and the label presence did not result in energy-friendly choices as hypothesized. This resulted in valuable design recommendations to improve the labels effects. To conclude, eye-tracking studies for domestic IoT labels could result in similar recommendations for improvements.

6.2. Strengths and Limitations

This study provides new contributions to research in the domestic IoT field. The combination of the factors included in this study, including security degree, framing, label type, initial attitude and trust in the label, and specifically looking into their interactions have not been done before and therefore provides valuable new insights.

To be more specific, security degree information has a considerable effect on purchase intention. In fact, among all factors included in this study, it has the strongest influence on purchase intention. Furthermore, framing effects on purchase intentions of domestic IoT included semantics, symbols and colours and examined their overall effect for two different label types, confirming again that positive framing has a positive effect on purchase intention.

The direct and moderating effects of trust in the label and initial attitude has, to the

authors knowledge, not been studied before in the context of IoT labels. This study contributes to the research by showing that trust and initial attitude have a strong influence on purchase intention, and considerably affect the uptake of security degree information.

Previous research on label type has focused on how differences in the design are perceived and judged (Emami-Naeini et al., 2019) and how they affect decision-making (Johnson et al., 2020). The current study more extensively explored how different label designs could affect purchase intention and found, contrary to previous research (Johnson et al., 2020), that label type does not affect purchase intention directly, but indirectly via trust in the label.

For the first study, the majority of participants were young, from Western Europe and university students so only a small fraction of the population interested in such devices and the findings of this study could thus not be generalized, especially since there is support for risk perception, attitudes towards smart devices, and purchase intention varying with age and education (Klobas et al., 2019; Shin, 2017). For the second study, this limitation was amended since participants of different ages and education level participated. The studies had largely the same findings, suggesting that different populations show similar patterns. However mainly people from the Western Europe participated in both studies which still makes generalizability to other countries, particularly beyond Western Europe, limited.

Moreover, the measure of trust pertained to the label itself, while trust in the information source, such as the manufacturer or the experts rating the security degree (who were not mentioned on the label), is also likely to affect trust in the information. Trust in the source has been found to facilitate behavioural change in accordance to the message (Ahluwalia, 2021). Trust in the source may further affect the purchase intention and should be included in further research as well.

In general, there are many kinds of domestic IoT devices, while this study only looked at smart speakers. Participants may give different responses for different types of smart devices which future studies could account for. For example, Zheng et al., 2018, found that individuals do not find smart devices, such as smart thermostats, as privacy invasive as devices that can record audio or visuals. Hence, it is likely that an informational breach of the former is perceived to be less severe and thus judged more kindly than the latter.

Furthermore, this study was based on a hypothetical scenario focusing on security information mostly and thus did not completely reflect actual purchase behaviour in real life. It did not include other relevant aspects influencing purchase decisions such as income, cost of the device, features of the smart device, or usefulness. To get the most accurate picture on

this decision-making process, one should include these as well. For example, Johnson et al., (2020) found that the willingness to pay for a smart device increases if a security label is present and van Deursen et al. (2021) found that not being able to afford domestic IoT leads to a more negative attitude, which in turn decreases the likelihood of purchasing. This implies that price and income play an important role as well. A discrete choice model is a common method to examine people's choices that can take multiple aspects into account and thus a good option for studying the effects of labels while accounting for other factors as well. Additionally, testing the effectiveness of labels in an actual shopping environment could also lead to different results in general.

Moreover, the data of study I (specifically framing being manipulated in a between-participants design) resulted in an ANCOVA being the most suitable form of analysis while a repeated measures would have been more suitable to account for order effects. Order effects were mitigated through randomization of security degree and framing order. With respect to label type, however, there was no randomization of the order; the grade variant was always shown first. The study can therefore not examine and control for the possible effect the order of presenting label types on decision-making. Nevertheless, the results of this study also indicate that label type does not have a significant direct effect on purchase intention and hardly moderates the effect of the other variables on purchase intention, because of which the order may not be of much importance. Still, we recommend future studies to completely randomize the order in which all labels are presented to rule out the influence of order effects on the findings of the study. Furthermore, the data was tested for possible order effects for framing and security degree and only one significant order effect for security degree has been found in study II. An additional variable was included in the analysis in order to control for this order effect. Despite these limitations, the current study provides valuable insights on the interrelated effects of security degree, label type, framing, initial attitude and trust in the label, tested in two samples.

6.3. Conclusion

Domestic IoT has been suffering from security and privacy issues for some time now and as awareness of these issues increases, so does the need of solving them. This study researched the way labels can contribute to this by nudging consumers' decision making into purchasing secure devices. It is also the first to systematically vary the label features reflecting security degree, framing and label type, and test their effects in interrelation with the psychological variables initial attitude and trust in the label. The conclusions, following a

survey with different label designs, are that information on security degree can steer behaviour towards purchasing more secure devices, in interaction with initial attitude and trust in the label. Initial attitude and trust in the label moderate the effect of security degree on purchase intention only to a limited extent, however, and are thus not strongly undermining the effectiveness of the label. Furthermore, positive framing directly increased purchase intention (and more strongly so for the grade label), as did a more positive initial attitude towards smart devices and more trust in the label. The study further showed that the informative label was more trusted, and since higher trust increases the effect of security level on purchase device, it seems that the informative label is more effective. Since more participants also prefer this label, this label seems to be the best choice. However, since there are also quite some consumers preferring the grade label as it is easier to understand for them, it might be best to combine both label types into one. Considering the importance of having safe devices in the home, and the strong impact of the security information on purchase intention in this study, we recommend that regulators make the use of security labels mandatory. We further recommend to make sure that trust in the label is high as that increases the effectiveness of the security information on the label in steering consumers towards purchasing safe devices.

References

- Ahluwalia, S. C., Edelen, M. O., Qureshi, N., & Etchegaray, J. M. (2021). Trust in experts, not trust in national leadership, leads to greater uptake of recommended actions during the COVID-19 pandemic. *Risk, Hazards & Crisis in Public Policy*, 12(3), 283-302. <https://doi.org/10.1002/rhc3.12219>
- Ajzen, I. (1985). *From intentions to actions: A theory of planned behaviour*. Springer
- Aleisa, N., Renaud, K., & Bongiovanni, I. (2020). The privacy paradox applies to IoT devices too: A Saudi Arabian study. *Computers & Security*, 96, 101897. <https://doi.org/10.1016/j.cose.2020.101897>
- Banks, S. M., Salovey, P., Greener, S., Rothman, A. J., Moyer, A., Beauvais, J., & Epel, E. (1995). The effects of message framing on mammography utilization. *Health Psychology*, 14(2), 178–184. <https://doi.org/10.1037/0278-6133.14.2.178>
- Bastos, D., Shackleton, M., & El-Moussa, F. (2018). Internet of things: a survey of technologies and security risks in smart home and city environments. In *Living in the Internet of Things: Cybersecurity of the IoT – 2018, 2018* (pp. 7). <https://doi.org/10.1049/cp.2018.0030>
- Block, L. G., & Keller, P. A. (1995). When to accentuate the negative: The effects of perceived efficacy and message framing on intentions to perform a health-related behavior. *Journal of Marketing Research*, 32(2), 192–203. <https://doi.org/10.1177/002224379503200206>
- Blythe, J., M., Johnson, S., D. (2018). *Rapid evidence assessment on labelling schemes and implications for consumer IoT security*. DCMS.
- Blythe, J. M., Sombatruang, N., & Johnson, S. D. (2019). What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?. *Journal of Cybersecurity*, 5(1), tyz005. <https://doi.org/10.1093/cybsec/tyz005>
- Bo, W., Zhang, Y., Hong, X., Sun, H., & Huang, X. (2014). Usable security mechanisms in smart building. In *2014 IEEE 17th International Conference on Computational Science and Engineering* (pp. 748-753). IEEE. <https://doi.org/10.1109/CSE.2014.154>
- Brass, I., Tanczer, L., Carr, M., Elsdon, M., & Blackstock, J. (2018). Standardising a moving target: The development and evolution of IoT security standards. *Living in the Internet of Things: Cybersecurity of the IoT* (pp.9). <https://doi.org/10.1049/cp.2018.0024>
- Cahenzli, M., Deitermann, F., Aier, S., Haki, K., & Budde, L. (2021). Intra-organizational nudging: designing a Label for governing local decision-making. In: Cuel, R., Ponte,

- D., Virili, F. (Eds). *Exploring Digital Resilience. ItAIS 2021. Lecture Notes in Information Systems and Organisation* (pp. 232–246). Springer.
https://doi.org/10.1007/978-3-031-10902-7_16
- Choe, E. K., Jung, J., Lee, B., & Fisher, K. (2013). Nudging people away from privacy-invasive mobile apps through visual framing. In Kotzé, P., Marsden, G., Lindgaard, G., Wesson, J., Winckler, M. (Eds). *Human-Computer Interaction – INTERACT 2013. Lecture Notes in Computer Science* (pp. 74-91). Springer.
https://doi.org/10.1007/978-3-031-10902-7_16
- Donovan, R. J., & Jalleh, G. (1999). Positively versus negatively framed product attributes: The influence of involvement. *Psychology & Marketing*, 16(7), 613-630.
[https://doi.org/10.1002/\(SICI\)1520-6793\(199910\)16:7<613::AID-MAR4>3.0.CO;2-F](https://doi.org/10.1002/(SICI)1520-6793(199910)16:7<613::AID-MAR4>3.0.CO;2-F)
- Emami-Naeini, P., Agarwal, Y., Cranor, L., F., Hibshi, H. (2020). "Ask the Experts: What Should Be on an IoT Privacy and Security Label?,"In *2020 IEEE Symposium on Security and Privacy (SP)* (pp. 447-464). IEEE.
<https://doi.org/10.1109/SP40000.2020.00043>.
- Emami-Naeini, P., Dixon, H., Agarwal, Y., & Cranor, L. F. (2019). Exploring how privacy and security factor into IoT device purchase behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1-12).
<https://doi.org/10.1145/3290605.3300764>
- European Commission (n.d.). *Energy savings*. Comissions.europa.
https://commission.europa.eu/energy-climate-change-environment/standards-tools-and-labels/products-labelling-rules-and-requirements/energy-label-and-ecodesign/about_en
- Festinger, L. (1957). *A theory of cognitive dissonance*. Stanford University Press.
- Frick, N. R. J., Wilms, K. L., Brachten, F., Hetjens, T., Stieglitz, S., & Ross, B. (2021). *The perceived surveillance of conversations through smart devices. Electronic Commerce Research and Applications*, 47, 101046. <https://doi.org/10.1016/j.elerap.2021.1010>
- Fridman, I., Glare, P. A., Stabler, S. M., Epstein, A. S., Wiesenthal, A., Leblanc, T. W., & Higgins, E. T. (2018). Information Framing Reduces Initial Negative attitude in Cancer Patients' Decisions About Hospice Care. *Journal of pain and symptom management*, 55(6), 1540-1545. <https://doi.org/10.1016/j.jpainsymman.2018.02.010>
- Gaspar, R., Luís, S., Seibt, B., Lima, M. L., Marcu, A., Rutsaert, P., ... & Barnett, J. (2016). Consumers' avoidance of information on red meat risks: information exposure effects on attitude and perceived knowledge. *Journal of Risk Research*. 19(4), 533-

549. <https://doi.org/10.1080/13669877.2014.1003318>
- Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & security*, 77, 226-261. <https://doi.org/10.1016/j.cose.2018.04.002>
- Ghiglieri, M., Volkamer, M., & Renaud, K. (2017). Exploring consumers' attitude of smart TV related privacy risks. In Tryfonas, T. (Eds). *Human Aspects of Information Security, Privacy and Trust: 5th International Conference, HAS 2017, Held as Part of HCI International 2017, Vancouver, BC, Canada, July 9-14, 2017, Proceedings 5* (pp. 656-674). Springer. https://doi.org/10.1007/978-3-319-58460-7_45
- Harkin, D., Mann, M., & Warren, I. (2022). Consumer IoT and its under-regulation: Findings from an Australian study. *Policy & Internet*, 14(1), 96-113. <https://doi.org/10.1002/poi3.285>
- Ho-Sam-Sooi, N., Pieters, W., & Kroese M. (2021). Investigating the effect of security and privacy on IoT device purchase behaviour. *Computer and Security*, 102, 102132. <https://doi.org/10.1016/j.cose.2020.102132>
- Jacobsson A., Boldt, M., & Carlsson B. (2016). A Risk Analysis of a Smart Home Automation System. *Future Generation Computer Systems*, 56, 719-733. <https://doi.org/10.1016/j.future.2015.09.003>
- Johnson, S. D., Blythe, J. M., Manning, M., & Wong, G. T. W. (2020). The impact of IoT security labelling on consumer product choice and willingness to pay. *Public Library of science*, 15(1). <https://doi.org/10.1371/journal.pone.0227800>
- Kanouse, D. E. (1984). "Explaining negativity biases in evaluation and choice behavior: theory and research", In Kinnear, T., C. (Eds). *NA - Advances in Consumer Research Volume 11, Provo, UT : Association for Consumer Research* (pp. 703-708).
- Karale, A. (2021). The challenges of IoT addressing security, ethics, privacy, and laws. *Internet of Things*, 15, 100420. <https://doi.org/10.1016/j.iot.2021.100420>
- Kelley, P. G., Cranor, L. F., & Sadeh, N. (2013). Privacy as part of the app decision-making process. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 3393-3402). <https://doi.org/10.1145/2470654.2466466>
- Keren, G. (2007). Framing, intentions, and trust-choice incompatibility. *Organizational Behavior and Human Decision Processes*, 103(2), 238-255. <https://doi.org/10.1016/j.obhdp.2007.02.002>
- Klobas, J. E., McGill, T., & Wang, X. (2019). How perceived security risk affects intention to use smart home devices: A reasoned action explanation. *Computers & Security*, 87,

101571. <https://doi.org/10.1016/j.cose.2019.101571>
- Laughlin, A. (2021, July 2) *How a smart home could be at risk from hackers*. Which. <https://www.which.co.uk/news/article/how-the-smart-home-could-be-at-risk-from-hackers-akeR18s9eBHU>
- Lebensmittelverband. (n.d.) *Nutri-Score system zur vereinfachten erweiterten Nährwerterkennung*. Lebensmittelverband. <https://www.lebensmittelverband.de/lebensmittel/kennzeichnung/naehrwert/nutri-score>
- Levin, I., P. (1987). Associate effects of information framing. *Bulletin of the Psychonomic Society*, 25(2), 85-86. <https://doi.org/10.3758/BF03330291>
- Levin I. P., & Gaeth, G. J. (1988). How consumers are affected by the framing of attribute information before and after consuming the product. *Journal of Consumer Research*, 15(3), 374 – 378. <https://doi.org/10.1086/209174>
- Maheswaran, D., & Meyers-Levy, J. (1990). The influence of message framing and issue involvement. *Journal of Marketing Research*, 27(3), 361–367. <https://doi.org/10.1177/002224379002700310>
- Petty, R. E., & Krosnick, J. A. (2014). *Attitude strength: Antecedents and consequences*. Psychology Press.
- Rosenblatt, D. H., Bode, S., Dixon, H., Murawski, C., Summerell, P., Ng, A., & Wakefield, M. (2018). Health warnings promote healthier dietary decision making: Effects of positive versus negative message framing and graphic versus text-based warnings. *Appetite*, 127, 280-288. <https://doi.org/10.1016/j.appet.2018.05.006>
- Rostami, A., Vigren, M., Raza, S., & Brown, B. (2022). Being Hacked: Understanding Victims' Experiences of {IoT} Hacking. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)* (pp. 613-631).
- Schuitema, G., Aravena, C., & Denny, E. (2020). The psychology of energy efficiency labels: Trust, involvement, and attitude towards energy performance certificates in Ireland. *Energy Research & Social Science*, 59, 101301. <https://doi.org/10.1016/j.erss.2019.101301>
- Shen, Y., & Vervier, P., A. (2019). IoT security and privacy labels. In Naldi, M., Italiano, G., Rannenber, K., Medina, M., Bourka, A. (Eds). *Privacy Technologies and Policy: 7th Annual Privacy Forum, APF 2019, Rome, Italy, June 13–14, 2019, Proceedings 7* (pp. 136-147). Springer. https://doi.org/10.1007/978-3-030-21752-5_9
- Shin, D., H. (2017). Conceptualizing and measuring quality of experience of the internet of things: Exploring how quality is perceived by users. *Information & Management*,

- 54(8), 998-1011. <https://doi.org/10.1016/j.im.2017.02.006>
- Sparks, J., & Ledgerwood, A. (2017). When good is stickier than bad: Understanding gain/loss asymmetries in sequential framing effects. *Journal of experimental psychology: General*, 146(8), 1086. <https://doi.org/10.1037/xge0000311>
- van Der Werff, L., Fox, G., Masevic, I., Emeakaroha, V. C., Morrison, J. P., & Lynn, T. (2019). Building consumer trust in the cloud: an experimental analysis of the cloud trust label approach. *Journal of Cloud Computing*, 8(1), 1-17. <https://doi.org/10.1186/s13677-019-0129-8>
- Van Deursen, A., J., van der Zeeuw, A., de Boer, P., Jansen, G., & van Rompay, T. (2021). Digital inequalities in the Internet of Things: differences in attitude, material access, skills, and usage, *Information, Communication & Society*, 24(2), 258-276. <https://doi.org/10.1080/1369118X.2019.1646777>
- Waechter, S., Sütterlin, B., & Siegrist, M. (2015). Desired and undesired effects of energy labels—An eye-tracking study. *Public Library of science*, 10(7). <https://doi.org/10.1371/journal.pone.0134132>
- White, M. P., Pahl, S., Buehner, M., & Haye, A. (2003). Trust in risky messages: The role of prior attitude. *Risk Analysis: An International Journal*, 23(4), 717-726. <https://doi.org/10.1111/1539-6924.00350>
- Zheng, S., Apthorpe, N., Chetty, M., & Feamster, N. (2018). User Perceptions of Smart Home IoT Privacy. *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW), 1–20. <https://doi.org/10.1145/3274469>

Appendix A

Attitude Scale

seven-point semantic differential

(1) negative – (7) positive

Please tell us what you think about using smart home devices in your own home in the future.

From my point of view, using a smart home device would be:

Foolish – Wise

Worthless – Valuable

Negative – Positive

A bad idea – A good idea

Unhelpful – Helpful

Appendix B

Grade Labels

Figure B1

Study 1 grade smart speaker label with low security degree and positive framing

Security Assessment - Protection and Security of the Device

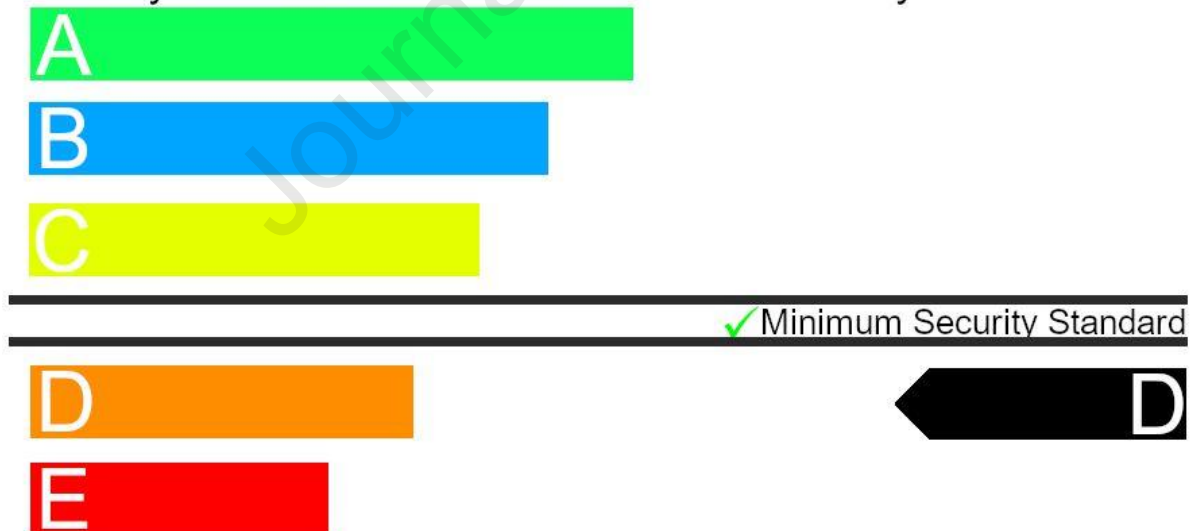


Figure B2

Study I grade smart speaker label with high security degree and negative framing

Security Assessment - Susceptibility and Vulnerability of the Device

**Figure B3**

Study I grade smart speaker label with low security degree and negative framing

Security Assessment - Susceptibility and Vulnerability of the Device

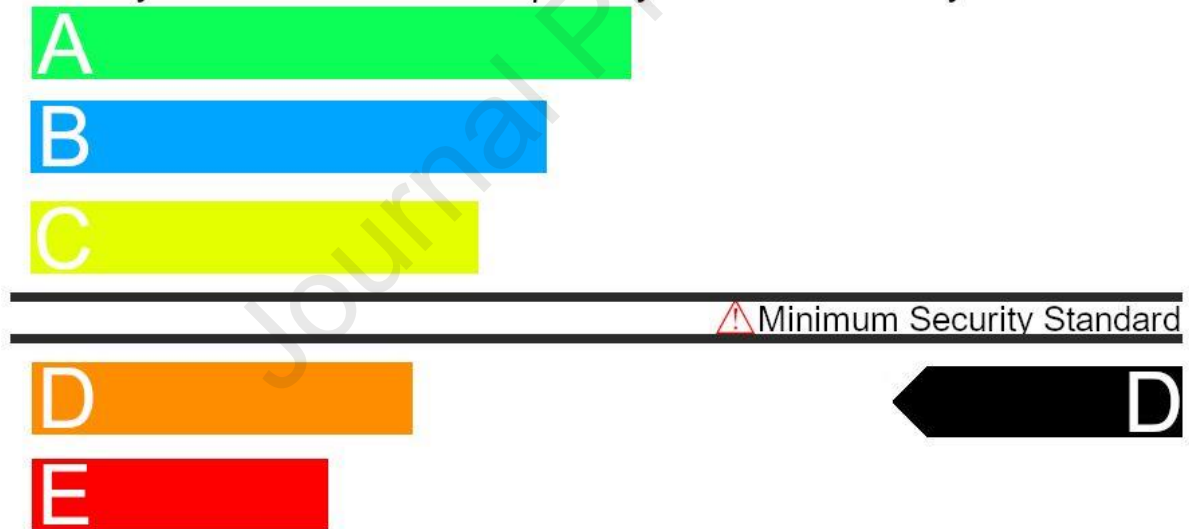
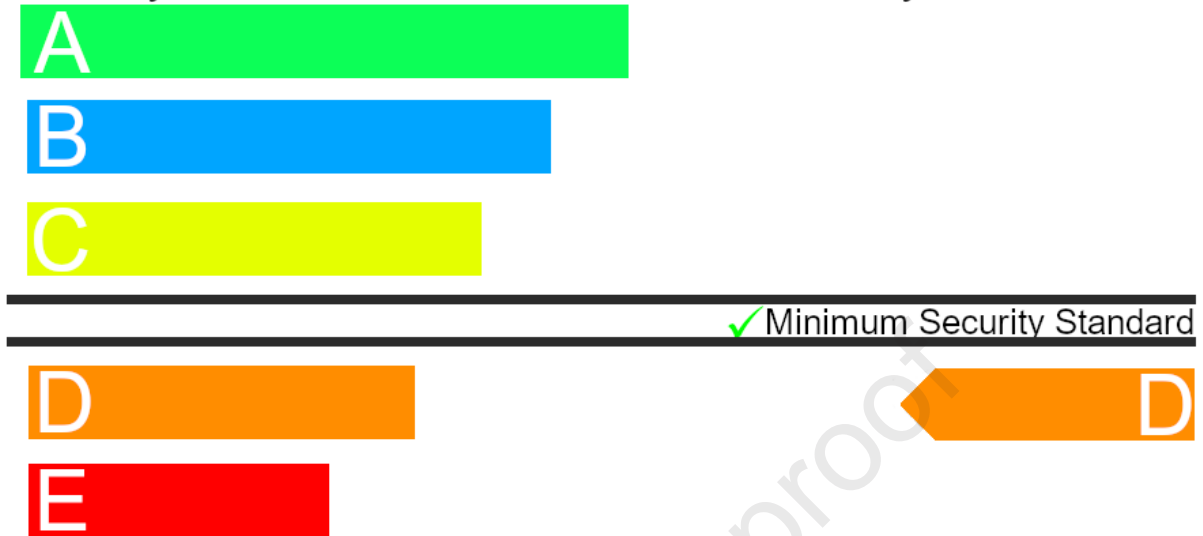


Figure B4

Study II grade smart speaker label with low security degree and positive framing

Security Assessment - Protection and Security of the Device

**Figure B5**

Study II grade smart speaker label with high security degree and negative framing

Security Assessment - Susceptibility and Vulnerability of the Device

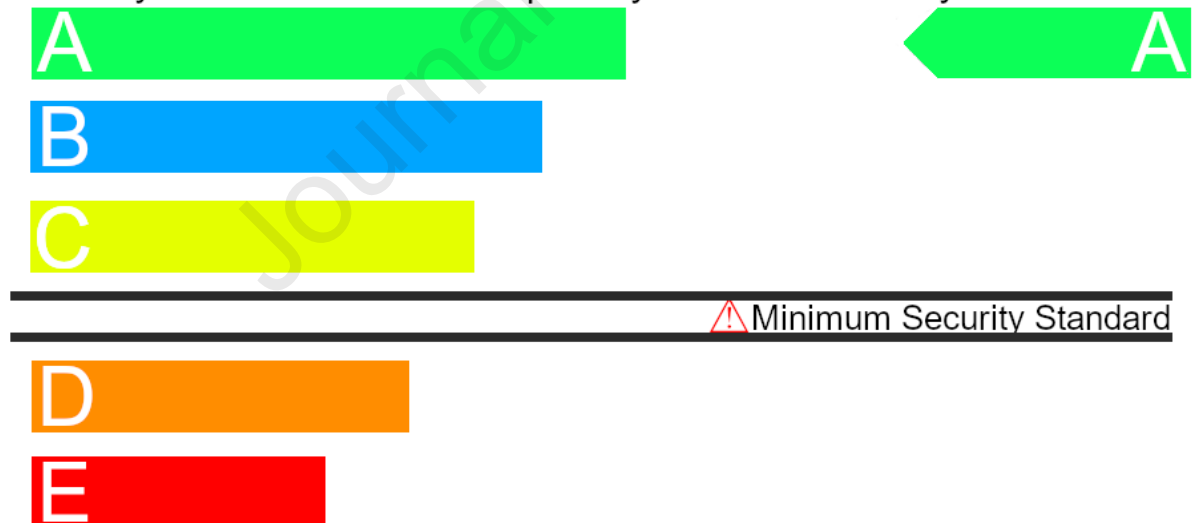
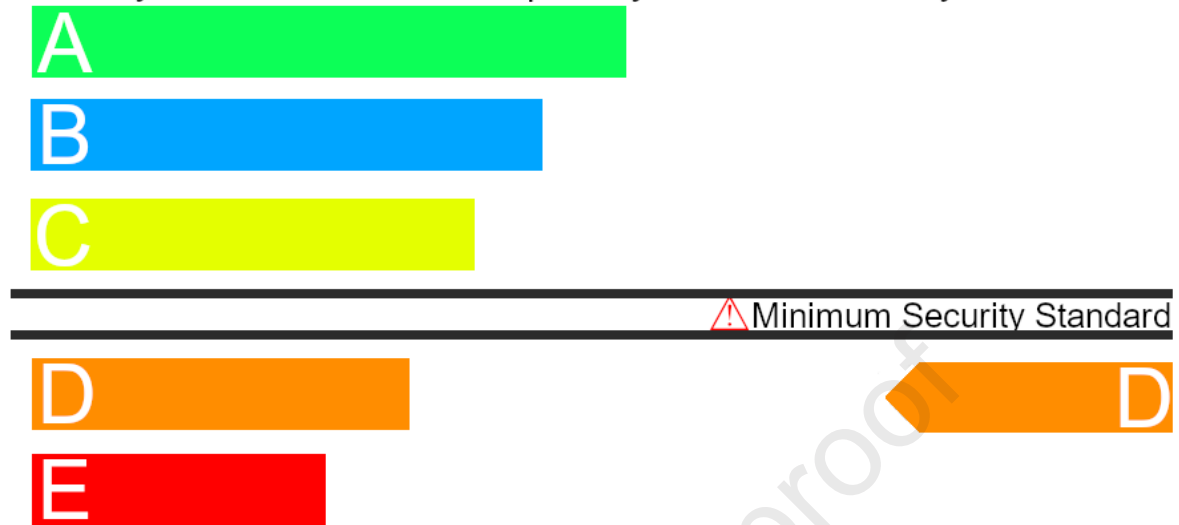


Figure B6

Study II grade smart speaker label with low security degree and negative framing


Security Assessment - Susceptibility and Vulnerability of the Device

Appendix C

Informative Labels

Figure C1


Study I informative smart speaker label with low security degree and positive framing

Security Assessment		
Protection and Security of the Device		
	Update*	Manual ✓
	Password*	No
	Authentication*	No
	Encryption*	No
	Internet access	Yes
	Connect to other devices	Yes

* required for minimum security standard

Figure C2


Study I informative smart speaker label with high security degree and negative framing

Security Assessment		
Susceptibility and Vulnerability of the Device		
	Update*	Automatic
	Password*	Default, updateable
	Authentication*	Two-factor
	Encryption*	Yes
	Internet access	Yes
	Connect to other devices	Yes

* required for minimum security standard

Figure C3


Study I informative smart speaker label with low security degree and negative framing

Security Assessment		
Susceptibility and Vulnerability of the Device		
	Update*	Manual
	Password*	No !
	Authentication*	No !
	Encryption*	No !
	Internet access	Yes
	Connect to other devices	Yes

* required for minimum security standard

Figure C4


Study II informative smart speaker label with low security degree and positive framing

Security Assessment		
Protection and Security of the Device		
Security 	Update*	Manual ✓
	Password*	No
	Authentication*	No
	Encryption*	No
	Internet access	Yes
	Connect to other devices	Yes

* required for minimum security standard

Figure C5


Study II informative smart speaker label with high security degree and negative framing

Security Assessment		
Susceptibility and Vulnerability of the Device		
Security 	Update*	Automatic
	Password*	Default, updateable
	Authentication*	Two-factor
	Encryption*	Yes
	Internet access	Yes
	Connect to other devices	Yes

* required for minimum security standard

Figure C6

Study II informative smart speaker label with low security degree and negative framing

Security Assessment		
Susceptibility and Vulnerability of the Device		
Security 	Update*	Manual
	Password*	No !
	Authentication*	No !
	Encryption*	No !
	Internet access	Yes
	Connect to other devices	Yes

* required for minimum security standard

Appendix D

Factor analysis of initial attitude study I and study II

Table D1

Factor loadings of initial attitude scale Study I

Item	Factor 1
Foolish-Wise	.782
Worthless-Valuable	.714
Negative-Positive	.765
A bad idea-A good idea	.738
Unhelpful-Helpful	.420

Table D2

Factor loadings of initial attitude scale Study II

Item	Factor 1
Foolish-Wise	.809
Worthless-Valuable	.827
Negative-Positive	.894
A bad idea-A good idea	.888
Unhelpful-Helpful	.816

Appendix E

Anova for study I to test homogeneity

Table E1

ANOVA with framing as dependent and gender, age, education, country as independent variable to test homogeneity

	<i>F</i>	<i>df</i>	<i>SS</i>	<i>p</i>
Gender	1.01	1,178	0.46	.181
Age	0.60	1,178	0.15	.438
Education	1.05	1,178	0.27	.308
Country	0.01	1,178	0.00	.916

Appendix F
three-way ANCOVA models for Study I and Study II

Table F1

Study I Three-way ANCOVA results for the direct effect of label type, framing, security degree, initial attitude and trust on purchase intention and additionally all two-way and some three-way interactions

	<i>F</i>	<i>df</i>	<i>SS</i>	<i>p</i>	ηp^2
<i>Model 3</i>					
Label Type (grade = 1)	1.55	1,763	2.46	.213	.002
Framing (positive = 1)	5.86	1,763	9.28	.016	.008
Security degree (high degree = 1)	1041.26	1,763	1649.16	<.001	.583
Initial attitude	94.23	1,763	94.23	<.001	.074
Trust	25.80	1,763	25.80	<.001	.021
Initial attitude*framing	.02	1,763	.03	.896	.000
Framing*security degree	.01	1,763	.02	.922	.000
Initial attitude*security degree	7.09	1,763	11.23	.008	.009
Initial attitude*framing*security degree	.88	1,763	.14	.767	.000
Framing*label type	.98	1,763	1.55	.322	.001
Initial attitude*label type	3.59	1,763	5.69	.058	.005
Initial attitude*framing*label type	.28	1,763	.45	.595	.000
Trust*label type	.01	1,763	.02	.907	.000
Trust*framing	1.79	1,763	2.83	.182	.002
trust*security degree	31.93	1,763	50.56	<.001	.041
Trust*initial attitude	1.03	1,763	1.63	.311	.001
Trust*security degree*initial attitude	.35	1,763	1.41	.346	.001
Trust*framing*initial attitude	.79	1,763	.11	.790	.000
R ²	.61				
ΔR^2	.03				

Table F2

Study I three-way ANCOVA results for the direct effect of label type, framing, security degree, initial attitude on trust and additionally all two-way and some three-way interactions

	<i>F</i>	<i>df</i>	<i>SS</i>	<i>p</i>	η^2
<i>Model 3</i>					
Label Type (grade = 1)	34.18	1,763	67.08	<.001	.044
Framing (positive = 1)	8.12	1,763	15.93	.005	.011
Security degree (high degree = 1)	7.05	1,763	13.84	.008	.009
Initial attitude	8.52	1,763	16.72	.004	.011
Initial attitude*framing	4.43	1,763	8.69	.036	.006
Framing*security degree	.48	1,763	.96	.485	.001
Initial attitude*security degree	78.92	1,763	17.52	.003	.012
Initial attitude*framing*security degree	.03	1,763	.07	.849	.000
Framing*label type	.74	1,763	.22	.738	.000
Initial attitude*label type	.19	1,763	3.33	.193	.002
Initial attitude*framing*label type	.26	1,763	.51	.608	.000
Security degree*label type	.05	1,763	7.56	.050	.005
R ²	.09				
ΔR^2	.08				

Table F3

Study II Three-way ANCOVA results for the direct effect of label type, framing, security degree, initial attitude and trust on purchase intention and additionally all two-way and some three-way interactions

	<i>F</i>	<i>df</i>	<i>SS</i>	<i>p</i>	η^2
<i>Model 3</i>					
Label Type (grade = 1)	2.45	1, 2223	3.79	.118	.001
Framing (positive = 1)	25.07	1, 2223	38.75	<.001	.011
Security degree (high degree = 1)	2569.93	1, 2223	3971.73	<.001	.538
Security order (high first = 1)	26.93	1,2223	41.61	<.001	.012
Initial attitude	272.43	1, 2223	421.02	<.001	.110
Trust	319.72	1, 2223	494.12	<.001	.127
Initial attitude*framing	1.02	1, 2223	1.58	.311	.000

Framing*security degree	2.07	1, 2223	3.20	.150	.001
Initial attitude*security degree	23.69	1, 2223	36.61	<.001	.011
Initial attitude*framing*security degree	3.12	1, 2223	4.83	.077	.001
Framing*label type	5.38	1, 2223	8.31	.020	.002
Initial attitude*label type	.04	1, 2223	.07	.830	.000
Initial attitude*framing*label type	2.00	1, 2223	3.09	.157	.001
Trust*label type	.94	1, 2223	1.46	.330	.000
Trust*framing	2.72	1, 2223	4.19	.099	.001
Trust*security degree	315.31	1, 2223	487.31	<.001	.125
Trust*initial attitude	1.13	1, 2223	1.74	.288	.001
Trust*security degree*initial attitude	.01	1, 2223	.02	.903	.000
Trust*framing*initial attitude	.20	1, 2223	.32	.652	.000
R ²	<hr/>				
	.65				
ΔR^2	.06				

Table F4

Study II Three-way ANCOVA results for the direct effect of label type, framing, security degree, initial attitude on trust and additionally all two-way and some three-way interactions

	<i>F</i>	<i>df</i>	<i>SS</i>	<i>p</i>	η_p^2
<i>Model 3</i>					
Label Type (grade = 1)	25.91	1, 2223	60.56	<.001	.012
Framing (positive = 1)	1.39	1, 2223	3.25	.238	.001
Security degree (high degree = 1)	29.72	1, 2223	69.45	<.001	.013
Initial attitude	44.16	1, 2223	103.18	<.001	.020
Initial attitude*framing	.43	1, 2223	1.02	.509	.000
Framing*security degree	.00	1, 2223	.00	.967	.000
Initial attitude*security degree	25.02	1, 2223	58.46	<.001	.011
Initial attitude*framing*security degree	.09	1, 2223	.21	.763	.000
Framing*label type	.18	1, 2223	.43	.667	.000

Initial attitude*label type	3.73	1, 2223	8.71	.054	.002
Initial attitude*framing*label type	.65	1, 2223	1.52	.421	.000
R ²	<hr/>				
	.06				
ΔR^2	.02				

Journal Pre-proof

Highlights

- Security degree information strongly affects purchase intention for smart speakers and trust in the label
- Positive framing has a small positive effect on purchase intention for smart speakers
- Label type does not affect purchase intention but does affect trust in the label with informative labels being more trusted
- Initial attitude and trust in the label moderate the effect of security degree on purchase intention

Journal Pre-proof

Declaration of interests

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.

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests:

Journal Pre-proof