

**Nudging Decision-Making for Purchasing Secure Domestic IoT: Labels and Framing  
Effects**

Michelle Walterscheid, s2154986

1<sup>st</sup> Supervisor: Nicole Huijts

2<sup>nd</sup> Supervisor: Iris van Sintemaartensdijk

Department Psychology of Conflict, Risk and Safety

Faculty of Behavioural, Management and Social Sciences, University of Twente

## **Abstract**

The domestic Internet of Things market is flooded with unsafe devices and there is little information available to differentiate them from safe ones. Still, the demand for domestic IoT rises as they increasingly get more affordable and convenient. This study aimed to find effective ways to affect decision-making of consumers in order to nudge them into purchasing safe devices. Multiple smart speaker labels were created and presented to participants to test the potential effects of differences in framing (positive vs. negative), security degree information (high vs. low) and label type (graded format vs. informative format) on purchase intention. Findings indicate positive significant effects for framing, security degree and initial attitudes on purchase intention but not for label type, as well as a positive interaction between initial attitudes and framing. Additional exploratory research found a positive and significant interaction effect between initial attitudes and security degree. Overall, information on security degree and framing can be used to nudge people to purchase safe smart devices.

## **Nudging Decision-Making for Purchasing Secure Domestic IoT: Labels and Framing Effects**

The domestic Internet of Things (IoT), more commonly known as smart devices, has been gaining popularity due to an increase in both acceptance and affordability (Ho-Sam-Sooi et al., 2021). In general, domestic IoT are devices linked within a network, usually to deliver a variety of services 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, watches or speakers to more entertainment-oriented ones like gaming consoles and TVs (Emami-Naeini et al., 2020). However, the rise in popularity revealed that domestic IoT devices have some serious security and privacy issues. To elaborate, many devices lack standard security features, especially cheap ones, which can be seen through the amount of hacker attacks suffered (Bastos et al., 2018). The lack of security is unfortunate since domestic IoT do have benefits that make them feasible such as improving well-being or supporting the disabled (Bastos et al., 2018). One reason for this issue is that consumers do not think about potential security and privacy issues before their purchase and thus do not look for it (Emami-Naeini et al., 2019). On top of that most information on security and privacy of smart devices is hard to find so even if consumers want to consider it, attempting to search for it takes too much effort. But, directly providing security information could enable consumers to incorporate security information in their decision-making. Researchers have already been examining the possibility of labels delivering this information, in order to raise the consumers awareness for security (Emami-Naeini et al., 2021; Emami-Naeini et al., 2020; Johnson et al., 2020; Shen & Vervier, 2019). Labels can be designed multiple ways and to ensure that they have the desired influence on purchasing behaviour, it is important to see which design works best to nudge decision-making into that direction. That is why this study seeks to identify label characteristics that can help with nudging behaviour to purchase safe devices.

### **Security and Privacy Issues**

In general, domestic IoT security suffers from issues such as unencrypted communication, weak authentication, or insufficient authentication (Bastos et al., 2018; Ho-Sam-Sooi et al., 2021). Many of these security problems occur since domestic IoT are connected to multiple devices within a network via Wi-Fi. The devices are susceptible to

communication being intercepted by hackers compromising the data. 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).

Information about privacy and security regarding the devices is often difficult to find and there are also many who do not concern themselves with the potential issues regardless of that (Emami-Naeini et al., 2019). The result of this lack of information is that users are often not quite aware of the security and privacy risks they expose themselves to. On top of that, most users trust the manufactures with collecting data, believing they will not misuse it as that would hurt their reputation or that regulators will prevent it (Tabassum et al., 2019). Furthermore, some users are not concerned with the privacy risks since they are used to sharing data that is collected to create targeted advertising. This is sometimes referred to as the privacy paradox: users have a tendency to both value privacy but still use IoT devices that lack privacy since they are just too convenient to give up (Emami-Naeini et al., 2020). A more general definition of the privacy paradox is that individuals claim to find privacy important but despite that do nothing to protect it (Ghiglieri et al., 2017).

The consequences of the lack of security ranges in severity. Hackers that gain access to domestic IoT can use the devices for botnets which can then be used for DDoS attacks or bitcoin mining, which is usually happens without the awareness of users. The hackers that have gained access of stored data can use it for forging data, blackmailing, extortion, or robbery as well (Jacobsson et al., 2016).

Various domestic IoT are also violating the privacy of the users. For example, smart speakers or other devices that activate after a certain phrase always have to listen for it, meaning they also hear private conversation and possibly record them as well (Karale, 2021). Generally, domestic IoT record user behaviour to be analysed by the manufacturers, but this information is sometimes sent without encryption giving individuals with malicious intent the opportunity to intercept this information and sell it. Additionally, usually the data that is being collected by domestic IoT is often times gathered without the users' consent. Moreover, some tracking devices can reveal the locations of users to the manufacturers at any time. That is especially problematic if the device is vulnerable towards cyberattacks, since hackers can use the location data, again to sell or use it themselves for robbery (Karale, 2021).

## **Interventions**

IoT devices have some serious security issues, despite calls for manufacturers to

provide more information on security and privacy. Some regulators want to improve the situation through standardized labels highlighting the best practices for products (Emami-Naeini et al., 2020). The content and presentation of standardized labels are determined by a pre-set guideline that would apply for every single domestic IoT product. The labels would offer information about the security status of smart devices, so that consumers can swiftly scan these labels, get a simple understanding on the security and compare them to other devices.

These kind of labels are already successfully used in other areas such as the food industry, using nutrition labels so that consumers can make choices based on nutritional values, and energy labels for choosing devices based on energy consumption (Rosenblatt et al., 2018; Schuitema et al., 2020). Some of these labels also use certain nudging techniques, such as framing. Framing the content of information in a negative or positive can be done in order to nudge decision-making into a certain direction. For example, negatively framed warnings on food products promote dietary control (Rosenblatt et al., 2018). Research on labels in the IoT area have already begun with Emami-Naeini et al. (2019) and Shen and Vervier (2019) creating prototypes of labels. They later also proposed which information in particular should be present on the labels, based on consumer and security expert interviews (Emami-Naeini et al., 2020). Johnson et al. (2020) already tested how labels affect decision-making and found that participants are likely to pick devices with labels over those without labels. However, there is still much room for exploration on how label design and its content can affect decision-making. To elaborate, there are different types of labels used in different industries to deliver information on products. Energy labels use a bar grading to grade energy efficiency. Some nutrition labels give a letter score from A to E, while others use the traffic light system (Blythe & Johnson, 2018), providing both exact nutrition numbers and indicating healthiness with the colours green, yellow and red. For now, developments in IoT labels focus more on informational tables, providing specific information on the devices' capabilities. The different label types have a trade-off between simplicity and complexity of information delivery. Which type best suits the domestic IoT context is to be determined.

Many countries only have just begun researching these issues and their potential solutions. The German government is conducting a research programme in early 2022, that considers developing standards, norms and certificates of safety. Additionally, in cooperation with the European union they work on a certificate scheme to be used as minimal security standard for broadband routers (BMBF, 2020; BSI, 2021). The Dutch government also finances research into possible certification and standardization methods (Tilburg University,

2019). But they also worked on interventions already, by running an informational campaign on the importance of updating smart devices (security.nl, 2020). They are also working on laws to be instated in early 2024, that would require manufacturers to reach a minimum standard to be permitted to sell their devices (Business.gov.nl, n.d.). Apart from that, the EU also mandates the usage of data protection impact assessments of privacy risks to be adhered to unless manufacturers are ready to pay a continuously increasing fine (Lodge & Crabtree, 2019). Lastly, the EU network for information security (ENISA) also has a report for best practices when it comes to privacy and security of IoT for manufacturers, however these are only recommendations and not mandatory (Shen & Vervier, 2019).

All in all, awareness of the security issues is rising, and research and interventions are underway to reduce sales of unsafe devices. However, the possibilities of labels are currently overlooked although they already have been effectively used in other industrial areas. But, since they are a new to the domestic IoT area, further research on how to best utilize them and to maximize their effectiveness is recommendable.

### **Psychological Mechanisms**

To ensure that labels have the desired effect of influencing purchase intentions towards safe devices, design practices, and psychological parameters that could improve or hinder its effectiveness should be explored. For the label design itself, label types can differ in their design and thus in how much information they present. It should be assessed which design is most appropriate as there is support that labels with more information can be difficult to understand, which should be avoided (Blythe & Johnson, 2018). Information on security, such as if it is high or low, is an important addition. While individuals value such information, it is usually difficult to find, but providing this information makes it more salient and easier to take into account influencing purchase intentions, possibly to avoid unsafe devices (Emami-Naeini et al., 2019). Additionally, framing could be used as a tool to nudge intentions towards, or away from purchasing domestic IoT, as it already has worked in the food industry (Rosenblatt et al., 2018). Lastly, individual attitudes towards domestic IoT and its security, is a prior influence on purchase intention that can affect effectiveness (reduce or improve) of other factors such as framing and thus its influence should be observed. All these concepts need to be examined more thoroughly first, before beginning the design process.

### ***Label Designs in IoT***

First and foremost, it is important to establish how, and which kind of information

should be presented on the label, to ensure that they have the desired effect on the individuals' purchase intentions. There are multiple label types that present information in different ways. Prominent examples are a grade label that grades the product according to a certain assessment scheme, as well as an informative label that includes an informative table. Specifically, informational labels often provide an exact description of the security and privacy measures in a text or table format which leads to it being the most descriptive of labels. This also makes it more difficult to understand, due to a tendency of using less known technical terms. Individuals not familiar with such terms, especially consumers with a low socioeconomic status have these issues (Blythe & Johnson 2018). Comparably, a grade label is easier to understand, simply grading the security using colours, letters, stars or bar length. Grade labels also have an additional effect on behaviour since the familiarity of well-known colour coding or letter ranking can invoke the affect heuristic leading to quick decision-making based on that familiarity (Blythe & Johnson 2018). However, when researching the impact of domestic IoT labels, the informative label was most effective at influencing participants choices towards secure devices and also the most preferred (Johnson et al., 2020). This would imply that the informative format is the most suitable choice for this study as well, but the grade label used in that study was originally designed for energy consumption information and not really adapted to fit the IoT context. To be specific, participants pointed out that the grading bars increasing in length as the grade worsens (which makes sense for the energy label as it indicates increased energy consumption) could be confusing since an increasing length would imply more and not less security. Adapting the energy label to properly fit into the domestic IoT area may lead to different outcomes. All in all, both the graded format and the informative format have their merits and disadvantages, with the former being simple to understand but lacking information and the latter providing that information but also being challenging to comprehend. Which one of the two works best still needs further exploration.

Now, when it comes to what kind of information should be incorporated into the label, information on the security level is a crucial addition. Individuals do value this type of information, but as of now it is difficult to find (Emami-Naeini et al., 2019). Furthermore, there is support that security information affects decision-making. For example, privacy ratings of apps, both general and from users, strongly influence decision-making on downloads (Choe et al., 2013). Low ratings made the apps seem less trustworthy and high ratings made them seem more trustworthy. Additionally, Kelley et al. (2013) found that displaying privacy permission information of apps on app stores influences the decisions of

users compared to app stores that do not display such information. Specifically, the added information results in choosing applications that are less privacy-invasive. While these studies pertain to privacy of the products, the same could apply with security, and could lead to people considering this information when choosing smart devices that have information on the security degree. Overall, security degree information should be incorporated into the label design, as it is likely to nudge purchase intention towards buying secure devices.

### ***Framing***

An additional method that helps with influencing individuals' decision-making is the way the content of the label is framed. Framing is a nudging technique utilizing differences in presentation of information such as certain colours, phrasing and images to unconsciously nudge individuals' decision-making into a more preferred direction (Choe et al., 2013). This method has the benefit that its influence is small but 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). Framing can be done through symbols (thumb-up vs. thumb-down), colours (green vs. red) or 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).

However, how to exactly utilize framing in order to nudge individuals away from unsecure domestic IoT is somewhat unclear. The type of framing to be used can depend on the desired behaviour to be reinforced and the context it is used in. For example, in the area of food production, negatively framed health warning messages are more effective than positive ones for nudging dietary self-control behaviours (Rosenblatt et al., 2018). When it comes to framed messages about the fat distribution of beef, positive (90% lean) framing increased attitudes towards the product compared to negative (10 % fat) framing (Donovan & Jalleh, 1999). Moreover, in the medical field, negative frames are more effective in eliciting preventive behaviours than positive frames. One suggested reason as to why negative framing has that effect is due to a negativity bias, leading to negative information having more weight than positive information (Kanouse, 1984). However, in an area more closely related to domestic IoT, positive framing of reviews and gradings was deemed to be more effective to



nudge users away from privacy-invasive apps than the negative framed ones (Choe et al., 2013).

When it comes to using framing on IoT labels, presenting information that is either positively or negatively framed, the study by Ho-Sam-Sooi, et al. (2021), in line with Choe et al. (2013) found that positive information about the gains of having more privacy and security is more effective to nudge adoption of preventive measures than negatively framed information. However, they warn that having a “pure” gain framing in this domain is difficult, since positive framing about security can still imply threats of attacks and thus are not truly about gain. It is also not certain if their results apply for purchase intention of domestic IoT the same way as it does preventive measures. All in all, previous research seems to indicate that negative frames are more likely to nudge individuals away from certain product, but there are exceptions to this rule.

### ***Initial Attitudes***

There are other factors, apart from the content or design of the labels, that can influence both purchase intention and the effectiveness of the label itself such as the initial attitudes towards domestic IoT. Initial attitudes are a crucial predictor of the willingness to both purchase and own domestic IoT (van Deursen et al., 2021). Specifically, the more positive the attitude is, the more likely it is that devices will be purchased. However, attitudes do not necessarily reflect actual behaviour. While attitudes towards smart devices tend to be negative, especially concerning security and privacy, people still frequently acquire them despite of that (Jaspers & Pearson, 2022). But, as mentioned previously, domestic IoT on the market often do not deliver much information on their privacy or security features, which may change attitudes.

Furthermore, It has been found that initial attitudes and framing interact with each other which could influence the effect of framing on decision-making. However, the outcome of that interaction seems to depend on the context. There are instances where framing that is congruent with initial attitudes results in a change of attitudes (Gifford & Bernard, 2006). But in other contexts, messages whose frames are incongruent will also result in such a change (Fridman et al., 2018). This is in line with the cognitive dissonance theory states that individuals become uncomfortable if their attitude does not match up with what they experience (Festinger, 1957). To reduce these feelings, individuals can either seek congruence by adapting their attitude and behaviour or avoid the information and thus dissonance (Gaspar et al., 2015). Park et al. (2020) find that individuals are more receptive to whatever framing is congruent with their attitude, arguing that their conclusion is supported through cognitive

dissonance, since individuals avoid the frame incongruent with their attitude. Apart from that research in other areas indicate that initial attitudes can bias the processing of information (van Strien et al., 2016). This bias is based on the tendency to reduce ambivalence between the perceived information and prior attitudes (Nordgren et al., 2006). Unfortunately, research on the interaction between initial attitude and framing in the IoT context is scarce. Due to this, it is hard to tell if and how the consumers attitude on IoT security can affect the effectiveness of framing. But the majority of studies in other contexts and cognitive dissonance theory itself would suggest that frames that match with the consumers initial attitude on smart devices are more likely to be accepted. In other words, the positive framing of a smart device's security combined with a positive initial attitude towards smart devices increases the likelihood to buy domestic IoT, while negative framing would decrease it. Consumers with negative attitudes are less likely to choose a smart device in general, and even more so with negative framing.

### **The current study**

The goal of this study is to find methods that nudge purchase intentions for domestic IoT away from unsecure devices. Due to this, the most important aspects suspected to affect purchase intention will be examined. First, the effectiveness of the specific label types will be assessed. Specifically, a label with a graded format, grading the device using letters, colours and bars, will be compared with a label with an informative format, listing security features in a table. Only one study examined the effectiveness of the grading format finding it somewhat effective, thus, this study aims to adapt the label type to better fit into the IoT context as well (Johnson et al., 2020). Secondly, the effect of negative vs. positive framing of information will also be examined, to see if framing can nudge consumers into buying more secure products. Thirdly, the inclusion of security information will also be addressed as that information is usually unavailable to customers and to identify what effect that additional information has on purchase intention. Lastly, initial attitudes of domestic IoT are a key factor to the intention of purchasing these devices. Initial attitudes are also likely to have an influence on framing, as such interactions have previously been observed in other research areas. Since this interaction has not been thoroughly researched in the domestic IoT context, it will also be examined in this study. Additional explorative measures are made, since the amount of data collected offers the opportunity examine the variables further. Specifically, looking at all the variables included in this study, some of their general effects and potential interactions between them (or the lack thereof) are yet unknown and thus should be examined.

Moreover, a previous study assessed opinions towards different label types and since this study also compares label types that differ from the first study, preferences will also be assessed (Johnson et al., 2020). In the end, the results of this study could be used to further adapt labels or could benefit the development of a standardized label scheme. With these goals in mind the following research questions and hypotheses are proposed:

**R1:** How does a grade label of security information affect decision-making (purchase intention) when purchasing domestic IoT compared to an informative label?

**R2:** How does the framing of the provided security information affect decision-making when purchasing domestic IoT and how do initial attitudes influence framing?

**H1:** Label type affects purchase intention (either positively or negatively).

**H2:** Positive framing has a positive effect on purchase intention.

**H3:** High security degree has a positive effect on purchase intention.

**H4:** Initial attitudes on smart home devices moderate the effect of framing on purchase intention.

## **Methods**

### **Participants**

To gather participants, convenience sampling was utilized by contacting local acquaintances working in the educational field, posting links on social media, and using the sona-system to recruit students. 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 ( $n = 9$ , with less than 75% completion) and lack of attention ( $n = 22$ ). Participants were randomly assigned to either the positive or

the negative framing group, resulting in 104 participants receiving negatively framed labels and 89 receiving positively framed labels. Two ANOVAs were executed to examine if gender and age are randomly distributed across the two framing groups. Both gender [ $F(3,193) = 1.01, B = .76, p = .388$ ] and age, [ $F(12,193) = .75, B = 2.28, p = .702$ ] are not significant, indicating that participants are indeed randomly distributed into the framing groups. The mean age of the participants was 21 ( $SD = 6.05$ ). Additionally, 24% ( $n = 47$ ) were male, 74% ( $n = 143$ ) were female, and 2% ( $n = 3$ ) either preferred not to say or chose an alternative option. The majority of the participant's nationality was centred around Europe with 53% ( $n = 102$ ) being Germans and 28% ( $n = 53$ ) being Dutch, while the other 19% ( $n = 38$ ) were scattered across Europe, Asia and America. Considering their educational level, 89% ( $n = 171$ ) finished high school, 4% ( $n = 8$ ) received a bachelor and another 4% graduated college ( $n = 8$ ). Fewest had either been to trade school (2%) or completed their PhD (1%). Moreover, participants were asked to indicate their knowledge on smart speakers to get a picture of their familiarity with domestic IoT. 47% ( $n = 91$ ) reported to know a moderate amount and 38% ( $n = 74$ ) knew a little and 8% ( $n = 15$ ) a lot. The rest of the participants indicated to either knew nothing at all (3%) or a great deal (4%). Lastly, this research project was approved by the BMS ethics committee of the University of Twente.

## **Design**

This study had a mixed design due to using both within and between variables (framing being between and all other variables being within). The independent variables are framing, initial attitude, label type, and security degree with purchase intention being the dependent variable. While framing, label type and security degree were determined by the label that was presented, initial attitudes and purchase intentions were measured per scale.

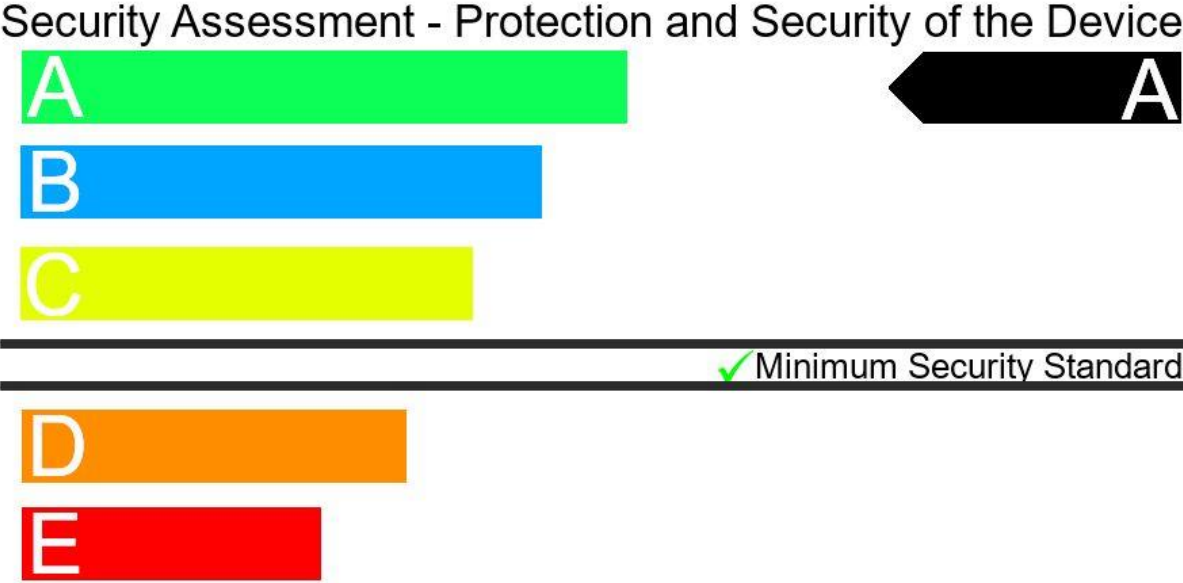
## **Materials**

Overall, eight different variations of labels were designed based on differences in label type, security degree and framing (see Appendix C and D). To elaborate, label type refers to the differences in presentation of information, that either being the grade format (Figure 1) or the informative format (Figure 2). The grade format grades security by letters going from A to E, colouring going from green to red as well as an increasing bar length if security is high and a decreasing length as security goes down. The informative format presents security

information in a table and lists the security measures. The table indicates if these measures are present and, if applicable, their capabilities. Next, labels could either indicate a low or a high degree of security either by the received grade for the graded label or per the number of security measures and their capabilities for the informative label. Framing was divided into positive and negative. Positive framing was conveyed using the colour green and checkmarks and negative framing used the colour red and exclamation points for informative labels and alert symbols for graded labels. For both label types, semantic framing was conveyed through different manners the shared sub-headers were phrased. The positively framed one stated:” protection and security of the device” to emphasize the advantages of security and the negatively framed stated: “susceptibility and vulnerability of the device” to emphasize the threats of lacking security.


**Figure 1**

*Graded smart speaker label with high security degree and positive framing*



**Figure 2**

*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

### ***Grade Label***

The grade label was based on the energy consumption label in use for electronic devices but adapted to fit into the IoT context (Figure 1). Since participants from the study by Johnson et al. (2020) 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 had been reached. This means that grades above C have the minimum amount of security features to be considered appropriate for this device, while a grade below implied that the device lacks certain important security features. This line was captioned as “minimum security standard” and was framed by either adding a green checkmark or a red alert symbol. Furthermore, the energy label has 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 this label had the length decrease to imply that security features are less present (Johnson et al., 2020 et al.; Choe et al., 2013). The number of grades were also shortened from A-G to A-E as the number of grades was also criticised to be too many (Johnson et al., 2020). This shortened range is also used on food products to grade nutrition and thus should be a bit closer to commonly known grade ranges.

### ***Informative Label***

The design and structure of the informative label are that of a table and were inspired by informative labels designed in previous research but shortened to mainly include information that is relevant for security (Emami-Naeini et al., 2020; Shen & Vervier, 2019). On the very left side symbols and headings indicated a security category, with the middle column defining the exact measures that the category includes (Figure 2). The very right column showed if the security measure was present and in case that a certain measure came with different capabilities, those were specified. Lacking features were negatively framed with the colour red and exclamation points while present features were positively framed through checkmarks and the colour green. Additionally, a minimum standard was given through the use of stars. Stars next to the features indicated which features are required to pass a minimum security standard which was mentioned in the footnote below the table. This was done to ensure that the two label types convey identical information as to not affect the decision-making.

## Measures

### *Initial Attitude*

Initial attitudes towards smart devices that specifically took security into account were measured with a slightly adapted scale initially used by Klobas et al. (2019) in their study about perceived security risks of smart home devices. It is a six item, seven-point semantic differential moving from extremely unlikely (1) to extremely likely (7) (see Appendix B). 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”. Overall, the maximum achievable score for attitude was 42 points, the minimum was six points, and the mean score was 25.44. The distributions among each subscale were assessed. Out of the six scales, three were slightly skewed to the left (worthless-valuable, bad idea-good idea, unhelpful-helpful). A factor analysis was also executed to assess if the items measuring initial attitudes do not measure multiple different factors. All conditions for factor analysis were met, the Kaiser-Meyer Olkin was above .06 (KMO = .867) Bartlett’s Sphericity was significant ( $p < .001$ ) and all item values were above .03. Only one factor was found, which implies the scale only measures initial attitudes towards smart speakers, so no items were removed from further analysis (Table 1). Lastly, the scale was also reliable ( $\alpha = 0.89$ ).

**Table 1**

*Factor loadings of initial attitude scale*

Item	Factor 1
Foolish-Wise	.894
Worthless-Valuable	.839
Boring-Exciting	.668
Negative-Positive	.884
A bad idea-A good idea	.877
Unhelpful-Helpful	.802

### *Purchase intention*

Purchase intention 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 are you to purchase the smart speaker based on its description?”, which was asked after each presentation of a label. The scale also included the question “Please pick extremely unlikely.”, to filter out participants that did not attentively fill out the survey. Distributions for the purchase intention of labels were examined showing that labels with a high security degree were skewed to the left and if the security degree was low it was skewed to the right. A summary of statistics is provided in the table below (Table 2). Displayed on it are the minimum, maximum and mean scores of purchase intention for all eight label variations.

**Table 2**

*Descriptive summary statistics of the difference in purchase intention based on label characteristics including, number of participants, minimum, maximum, mean and standard deviation of purchase intention*

<b>Label characteristics</b>	<b>Framing</b>	<b>N</b>	<b>Minimum</b>	<b>Maximum</b>	<b>Mean</b>	<b>S.D</b>
Graded, high-security	Positive	89	1	7	4.75	1.58
Graded, low-security	Positive	89	1	5	2.01	1.02
Informative, high-security	Positive	89	1	7	5.03	1.55
Informative, low-security	Positive	89	1	6	1.91	1.21
Graded, high-security	Negative	102	1	7	4.68	1.73
Graded, low-security	Negative	104	1	5	1.77	.94
Informative, high-security	Negative	102	1	7	4.66	1.71
Informative, low-security	Negative	102	1	5	1.66	.95

## **Procedure**

An English online survey was created using Qualtrics in order to collect data (see Appendix E). First, instructions explaining the aims and content of the survey as well as ensuring that participants can quit participating at any point in time were presented. In addition to that, the informed consent form was also shown to acquire consent. Participants also 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 kept anonymous and confidential to keep it private. Afterwards, demographics were collected including: age, gender, country of



birth, educational level and initial attitudes towards security of smart devices. This was followed by a general explanation of smart devices and their capabilities, so that participants that are not familiar with smart devices can still participate. The participants were presented with the scenario that they are looking to buy a smart speaker device, which was followed by the instruction that smart speakers will be shown to them one after another and 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 (Figure 1), grading the security by colouring, letter and bar length. The last two labels were informative (Figure 2), presenting a table listing security features. 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. However, the order of presented label types remained as to not confuse participants with switching the formats back and forth. While being presented with the label, participants were asked the question that measured purchase intention. At the end participants could voluntarily choose which label type they preferred and add a reason as well. Afterwards they got a short debriefing of the study goals and were thanked for their participation. Participants recruited from the sona-system were rewarded with a quarter of a credit.

## **Analyses**

The programmes SPSS (version 25) and Jamovi (version 2.2.5) was used for the statistical analysis of the data. Additionally, distributions for initial attitudes and purchase intention were also assessed. Moreover, for the first three hypotheses an ANOVA with the variables label type, framing and security degree was executed to examine the effect of the variables on purchase intention. For the fourth hypothesis a two-way ANCOVA was conducted. Additionally, exploratory analyses were executed resulting in one three-way ANCOVA model as well as a contrast analysis. Lastly, written responses about label preferences were coded inductively.

## Results

In order to test the first three hypotheses an ANOVA model was conducted including the variables label type, framing and security degree as independent variables and purchase intention as dependent variable (Table 3). For the first hypothesis that label type affects purchase intention, no significant effect between the two variables was found and thus no support for the first hypothesis. Concludingly, label type does not influence the purchase intention of smart speakers. For the second hypothesis that positive framing has a positive effect on purchase intention, a significant and positive effect of framing on purchase intention was found. Hence, positive framing increases the purchase intention of smart speakers. For the third hypothesis that a high security degree positively affects purchase intention a strong positive significant effect of security degree on purchase intention was found. In other words, a high security degree greatly increases purchase intention of smart speakers. To conclude, support for hypothesis two and three was found but not for hypothesis one.

**Table 3**

*ANOVA results for the effect of label type, framing and security degree on purchase intention including F-value, degrees of freedom, effect size and significance*

	<i>F</i>	<i>df</i>	<i>B</i>	<i>p</i>
Label type (graded = 1)	.23	1, 766	.45	.630
Framing (positive = 1)	5.93	1, 766	11.38	.015
Security degree (high degree = 1)	839.699	1, 766	1612.32	<.001

R Squared = .53 (adjusted R Squared = .52)

For the fourth and last hypothesis, that initial attitudes moderate the effect of framing on purchase intention, a two-way ANCOVA was executed with initial attitudes, framing and their interaction as independent variables and with label type and security degree added as control variables. A positive significant interaction between initial attitudes and framing on purchase intention was found, supporting the hypothesis (Table 3). Specifically, initial attitudes have a more positive effect on purchase intention if framing is positive rather than negative (Figure 4). Additionally, initial attitudes by themselves also have a positive effect on purchase intention, indicating that positive initial attitudes increase the purchase intention of smart speakers.

**Table 3**

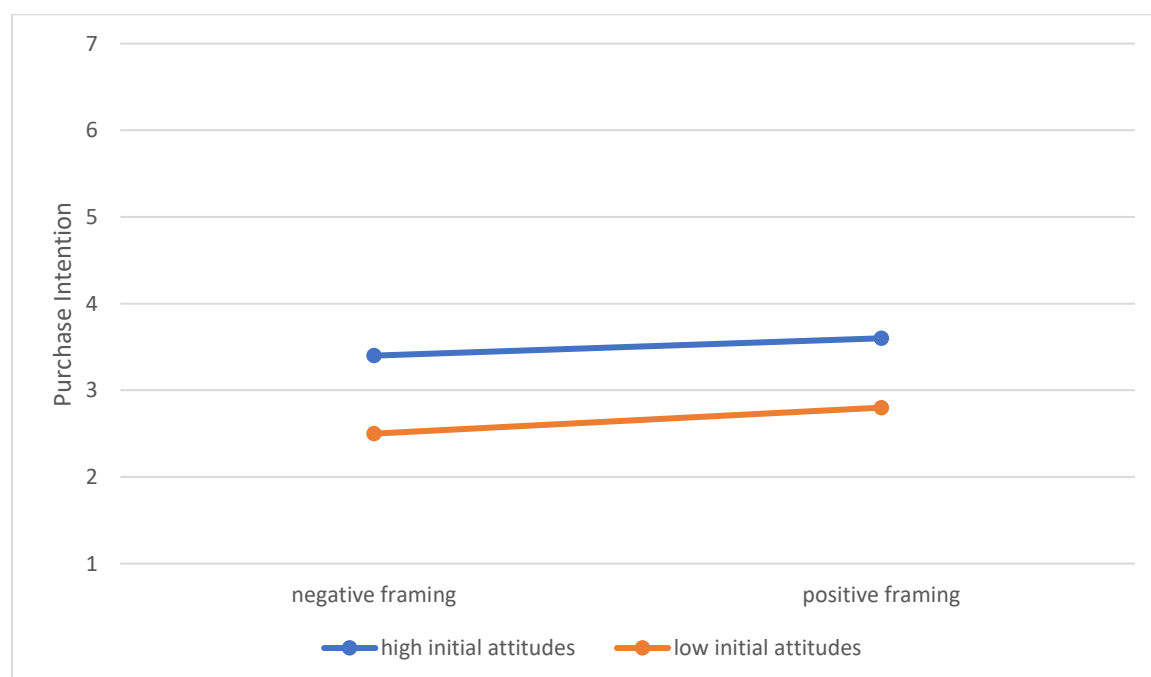
*Two-way ANCOVA results for the interaction effect of initial attitudes and framing on purchase intention including F-value, degrees of freedom, effect size and significance*

	<i>F</i>	<i>df</i>	<i>B</i>	<i>p</i>
Label Type (graded = 1)	.30	1, 766	.50	.586
Framing (positive = 1)	4.86	1, 766	4.86	.089
Security degree (high degree = 1)	962.47	1, 766	1613.14	<.001
Initial attitudes	3.69	32, 766	198.05	<.001
Initial attitudes*framing	1.56	24, 766	62.90	.042

R Squared = .09 (adjusted R Squared = .02)

**Figure 4**

*Significant interaction effect between initial attitudes and framing on purchase intention*



### **Qualitative research: Label preferences**

Participants were asked to indicate their preferences of the label types and could voluntarily add a reason for their decision. The responses were inductively coded, resulting in the following codes: ‘easy to understand’, ‘colours’, ‘simplicity’, ‘more information’ and ‘detail’. To summarize, 74% ( $n = 143$ ) preferred the informative format, while 19% ( $n = 37$ )

preferred the graded 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.”), (graded  $n = 14$ , e.g. “To me it is more understandable and I like visualizations with colours most.”).

### Exploratory analyses

An additional three-way ANCOVA model was executed including all variables measured in this study to explore if unexpected interaction effects exist (Table 5). Especially of interest was if label type may have significance in interactions with other variables and if security degree has other interactions since a strong and significant effect was found previously. No significant interactions with label type and any other variable were found, but initial attitudes and security degree were found to have a significant positive interaction. Contrast analysis revealed that while low initial attitudes increased purchase intention  $t(753) = 18.7, p < .001$ , high initial attitudes increased purchase intention more  $t(753) = 24.6, p < .001$ . To elaborate, a high security degree has a stronger positive effect on purchase intention if the initial attitudes are high rather than low (Figure 4).

**Table 5**

*Three-way ANCOVA results for the interaction effect of initial attitudes, degree of security and framing on purchase intention including F-value, degrees of freedom, effect size and significance*

	<i>F</i>	<i>df</i>	<i>B</i>	<i>p</i>
Label Type (graded = 1)	.15	1, 766	.25	.698
Framing (positive = 1)	2.93	1, 766	4.85	.088
<b>Security Degree (high degree = 1)</b>	<b>500.47</b>	<b>1, 766</b>	<b>828.52</b>	<b>&lt;.001</b>
<b>Initial attitudes</b>	<b>3.74</b>	<b>32, 766</b>	<b>198.16</b>	<b>&lt;.001</b>
<b>Initial attitudes*framing</b>	<b>1.60</b>	<b>24,766</b>	<b>63.25</b>	<b>.037</b>

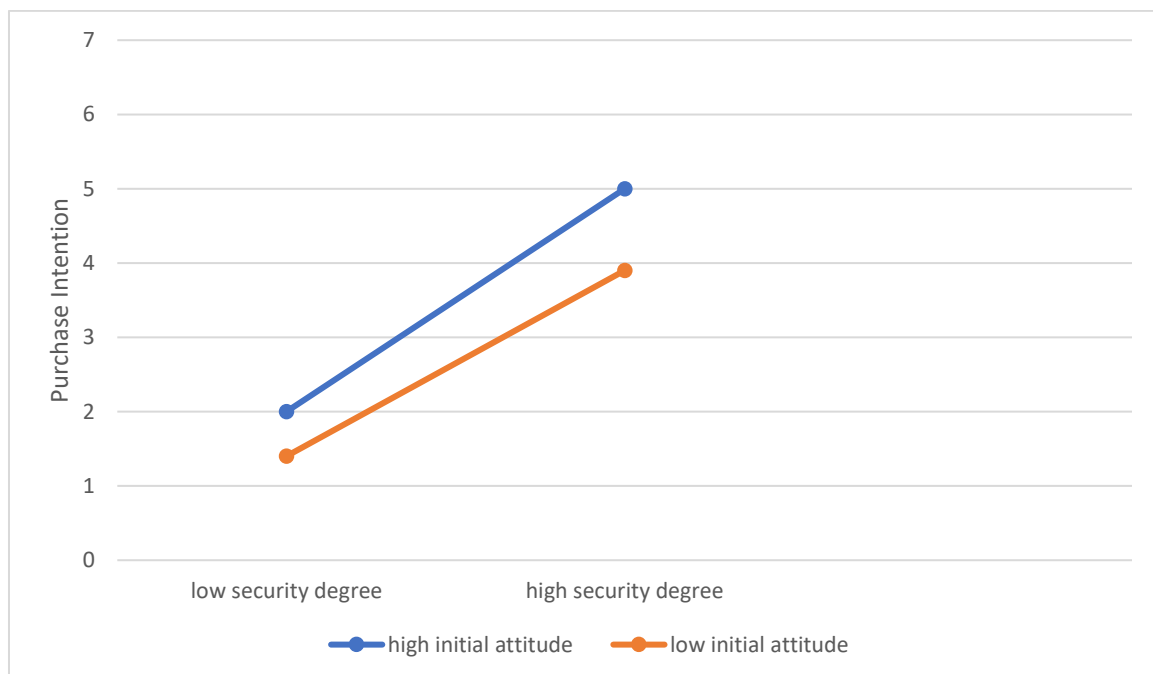
Framing*security degree	.02	1,766	.03	.902
<b>Initial attitudes*security degree</b>	<b>1.79</b>	<b>32,766</b>	<b>94.77</b>	<b>.005</b>
Initial attitudes*framing*security degree	1,21	23,766	49,84	.153
Framing*label type	.27	1,766	.46	.599
Initial attitudes*label type	.67	32,766	35.59	.916
Initial attitudes*framing*label type	.38	23,766	14.52	.996

R Squared= .68 (Adjusted R Squared= .59)

Note. significant results are in boldface

#### Figure 4

*Significant interaction between initial attitudes and security degree on purchase intention*



### Discussion

The goal of this study was to develop and examine different label designs in order to find methods that could nudge consumers to purchase safe smart devices. To achieve this goal multiple labels with varying features were created. One such feature was the label type divided into a grade format that only graded security from A to E and an informative format which presented a table that showed which security features were present. Another was the framing of the information, positive framing was done via checkmarks, the colour green and an emphasis on protection while negative framing was through alert symbols and exclamation points, the colour red and an emphasis on susceptibility. Lastly, labels differed in the level of

security they represent. Some labels indicated that devices lack security, while others indicated the opposite. Participants indicated their intention to purchase domestic IoT based on the labels and their initial attitudes on the devices in general was also assessed.

The first hypothesis assumed that there would be a difference in purchase intention based on the label type presented, but no significant effect was found. However, qualitative research on preferences of label types indicated that participants preferred the informative type over the grade type. The second hypothesis that positive framing has a positive effect on purchase intention could be supported, albeit the effect of framing was very small. The third hypothesis about information about the degree of security of the smart devices had the strongest impact on purchase intention variables. Consumers are much more willing to purchase devices with a high security degree, compared to devices with low security. Additional explorative research found a positive interaction between security degree and initial attitudes on purchase intention. The final hypothesis about positive initial attitudes having an interaction with framing on purchase intention could also be supported. Additionally, the higher the initial attitudes are the more positively they affected purchase intention.

## **Findings**

That no support could be found for label types affecting purchase intention could imply that the formatting of the smart speakers' information has no effect on the decision-making process to purchase domestic IoT. Other aspects of the label's design seem to have greater salience, as can be seen by the effects of framing and security degree. However, even though no explicit effect of the label type was found to influence purchase intention, qualitative analysis showed that the great majority of the participants do have a preference for the informative type over the graded type. In the study by Johnson et al. (2020), participants also preferred the informative label type, although the difference between preferring the grade label and the informative label is much smaller compared to this study. Participants in their study also stated that they disliked the lack of information of the graded label, which is also the case for this study. This indicates that individuals value security information and would prefer it to be present. If participants actually use it is another matter, since the privacy paradox also indicated that individuals tend to not act on that. However, most security information with these previous results was hard to find. Perhaps by providing this information directly, individuals will take it more into consideration.

Moving on, support for framing affecting purchase intention has been found but the effect is very small. The study of Choe et al. (2013) that examined framing but in connection with app stores and privacy invasive-apps also concluded that its effect is subtle, finding that positively framed icons of privacy ratings resulting in apps being viewed unfavourably. Similarly, the study of Ho-Sam-Sooi, et al. (2021) found that the gain framed information (using semantics) about the gains of having more privacy and security is more effective to nudge the adoption of preventive measures. Contrary to these results, this study finds that negatively framed information (using semantics, colours and symbols for framing) about security is more effective to nudge consumers away from purchasing smart devices in general. The reason for this difference is somewhat unclear. While there are exceptions, negative framing usually results in a deterrent effect, which this study can support (Kanouse, 1984). Besides, that the study by Choe et al. (2013) only used icons for framing and also had the context of privacy-invasive apps. The difference in context of domestic IoT and the different layers of framing could be a reason for this difference. For Ho-Sam-Sooi et al. (2021) the context is the same, but their message was phrased differently compared to this study. Their messages were strictly about gains or losses, stating that devices are either secured or that they can be hacked while this study is more vaguely talking about either protection or susceptibility of the device. The results of this study support that framing can be used to nudge consumers intentions away or towards purchasing smart speakers, but that effect is very small.

The most crucial of the finding is that information about the degree of security of the smart devices has a strong impact on purchase intention. Consumers are much more willing to purchase devices with high security, compared to devices with low security and that is independent of the presentation (graded vs. informative) of that information. Emami-Naeini et al. (2019) found that consumers looking to purchase smart devices consider privacy and security information but are troubled by that information being hard to find. The researchers also add that consumers find this kind of information important and providing could lead to being incorporated in the decision-making process to purchase the devices, which this study can support since security degree information had a strong impact on purchase intention. Thus, providing information on the security degree could indeed deter consumers from purchasing unsafe devices, instead opting for safer alternatives.

Additionally, exploratory research found an interaction effect between initial attitudes and security degree on purchase intention. Initial attitudes seem to have a more positive effect on purchase intention if the security degree is high rather than low. Strong attitudes have a

tendency to be more stable and resistant to persuasion (Petty & Krosnick, 1995). This could explain why individuals with very positive initial attitudes still have higher purchase intentions despite a low security degree compared to participants with negative initial attitudes.

Initial attitudes towards smart devices, also affect purchase intention. This effect is stronger than the framing effect but not as strong as the one of security degree and shows that the more positive initial attitudes are, the higher is the purchase intention. This is supported by theories of technology acquisition that state that negative attitudes decrease the likelihood of acquiring or owning IoT devices, while positive attitudes increase the likelihood of it (van Deursen et al., 2021). It was hypothesized that initial attitudes and framing would interact together in influencing purchase intention. The findings support that initial attitudes have a more positive effect on purchase intention if framing is positive rather than negative. This seems to be in line with the study of Park et al. (2020), who found individuals to be more receptive to whatever framing is congruent with their attitudes, since purchase intentions strongly increase with both positive initial attitudes and positive framing, but not so much with negative attitudes and positive framing. This would mean that framing would have the strongest effect if it matches with attitudes, making it less feasible in other cases.

All in all, label type made no difference towards purchase intentions, while framing, security degree and initial attitudes did. Consumers were more willing to purchase smart devices if framing is positive and security degree and initial attitudes are high, compared to when framing is negative and security and initial attitudes are low. Lastly, security degree and framing matching with initial attitudes lead to stronger intentions, either for or against purchasing smart speakers.

## **Limitations**

Although this study was open for anyone interested, the majority of participants were young, from Europe and university students so only a small fraction of the population interested in such devices and thus should not be generalized. Especially, since there is support for purchase intention varying with age and education. When comes to smart devices, the young and less educated take their security risk perception less into account in their decision making, compared to the old and more educated (Klobas et al., 2019). Younger individuals also tend to have more positive attitudes towards smart devices and their attitudes have a stronger effect on their purchase intention. For example, Shin (2017) found that the



young have more positive attitudes towards smart watches and that their attitude influences their purchase intention strongly.

Moving on, this study's main focus was on the effect that different label designs, specifically the variations of framing, security degree and label type have on purchase intention and thus did not include other relevant aspects of such a purchase such as price or usefulness. However, to get the most accurate picture on this decision-making process, one should include these as well. To specify, van Deursen et al. (2021) state that not being able to afford domestic IoT leads to a more negative initial attitude and so decreases the likelihood of purchasing and also implies that price and income play a role. The number of different labels presented and designed is still a good addition to the research literature as that has not been done very often. Additionally, the inclusion of initial attitudes and its relation to security and framing is also a unique addition and has not been explored much in the domestic IoT realm before.

## **Future research**

As mentioned before, although label type does not seem to influence purchase intention, participants did have a clear preference for the informative type compared to the graded one. The stated reason for the preference of each label seems to have been based on the individuals' knowledge on smart devices. Those preferring the graded format did so due to its simplicity and having trouble understanding the informative one, while the informative type was preferred for going into detail. Thus, perhaps knowledge and understanding of smart devices could influence purchase intention based on different label types.

Additionally, since this study only examined the effect of either positive or negative framing, examining the effect of mixed framing that has both positive and negative aspects or no framing at all could also be done in order to compare potential changes in the effect on purchase intention. Moreover, the security degree was also limited to a very high degree of security and a very low degree, but no medium degree or others in between were included. More variety and its effect on purchase intention should be researched, taking initial attitudes into account. This study also only included security and left out privacy. While these two concepts have some overlap, privacy should also be given individual attention to ensure that the effects found here for security are also similar to privacy.

Lastly, as mentioned before, this study's population mainly consisted of local university students and thus represent only a part of the research population. Due to this, a

repetition of this study but with a more diverse set of people would be appropriate to get a more accurate view of attitudes and the effect of label characteristics such as framing or security degree.

### **Design recommendations**

From the results of the study, a few suggestions for future designs of domestic IoT labels are summarized that could encourage consumers to purchase smart devices that have a high security standard. One of the most important things to add is a form of security rating as that has shown to have a strong influence on purchase intention. This ranking should be in a form most familiar with the population such as stars or an A-E grading so that a quick glance is enough to tell the device's safety (Blythe & Johnson 2018). A low security rating greatly decreases the willingness to purchase devices while a high security rating can increase it. Moreover, framing can be implemented on labels through general colouration (red vs. green), symbols (alert icon vs. checkmark) and wording (susceptibility vs. protection). If labels should implement framing is debatable as the effect is very small, and it also seems that negative framing would lower purchase intention regardless of security degree. If the intention is for consumers to be slightly more sceptical of devices in general, negative framing is a possible option, if one wants to increase purchase intention by a small margin, then positive framing can be used. Lastly, for label types, this study could not confirm that different types influence purchase intention. However, it is perhaps best to create a design that combines both, informative and graded aspects such as an informative table with detailed information including a section for a grading using letters or stars. Through that, consumers can both easily understand and compare devices but also get all the details so knowledge on domestic IoT does not matter as much (Blythe & Johnson, 2018).

### **Conclusion**

Domestic IoT have 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. The conclusions, following a survey with different label designs, are that information on security degree and framing can affect purchase intention. Specifically, positive framing and high security degree increase purchase intention while

negative framing and low security degree decrease purchase intention, although initial attitudes towards smart devices moderate those effects to a certain degree. In the future, governments could enforce laws so that manufacturers incorporate these label designs in order to nudge consumers to purchase safer smart devices.

## References

- Bastos, D., Shackleton, M., & El-Moussa, F. (2018). Internet of things: a survey of technologies and security risks in smart home and city environments. *Living in the Internet of Things: Cybersecurity of the IoT*, 1-7. <https://doi.org/10.1049/cp.2018.0030>
- Blythe, J., M., Johnson, S., D. (2018). *Rapid evidence assessment on labelling schemes and implications for consumer IoT security*. DCMS.
- BMBF. (2021, June 2). *Bekanntmachung*. Retrieved 2021, November 26 from: [https://www.bmbf.de/bmbf/shareddocs/bekanntmachungen/de/2021/06/3642\\_bekanntmachung](https://www.bmbf.de/bmbf/shareddocs/bekanntmachungen/de/2021/06/3642_bekanntmachung)
- BSI. (2021). *Die Lage der IT-Sicherheit in Deutschland*. Bundesministerium für Inneres und Heimat. [https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-cybersicherheit2021.pdf?\\_blob=publicationFile&v=3](https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-cybersicherheit2021.pdf?_blob=publicationFile&v=3)
- Business.gov.nl. (n.d.). *Security of smart devices must be improved*. Retrieved 2022, January 15 from <https://business.gov.nl/amendment/improving-security-smart-devices/>
- Cahenzli, M., Deitermann, F., Aier, S., Haki, K., & Budde, L. (2021). Intra-Organizational Nudging: Designing a Label for Governing Local Decision-Making. *XVIII Conference of the Italian Chapter of AIS - Digital Resilience and Sustainability: People, Organizations, and Society*.
- Choe, E. K., Jung, J., Lee, B., & Fisher, K. (2013). Nudging people away from privacy-invasive mobile apps through visual framing. In *IFIP Conference on Human-Computer Interaction* (pp. 74-91). Springer.
- 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/10.1.1.1039.7462>
- Emami-Naeini, P., Agarwal, Y., Cranor, L., F., Hibshi, H. (2020). Ask the Experts: What should be on an IoT privacy and security label? *2020 IEEE Symposium on Security and Privacy*, 447. <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. *Conference on Human Factors in Computing Systems – Proceedings*, 1-12. <https://doi.org/10.1145/3290605.3300764>
- Festinger, I. (1957). *A theory of cognitive dissonance*. Stanford University Press.
- 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 Attitudes 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 attitudes and perceived knowledge. *Journal of Risk Research*. 19(4), 533-549. <https://doi.org/10.1080/13669877.2014.1003318>
- Ghiglieri, M., Volkamer, M., & Renaud, K. (2017). Exploring consumers' attitudes of smart TV related privacy risks. *Human Aspects of Information Security, Privacy and Trust*, 656-647. [https://doi.org/10.1007/978-3-319-58460-7\\_45](https://doi.org/10.1007/978-3-319-58460-7_45)
- Gifford, K., & Bernard, J. C. (2006). Influencing consumer purchase likelihood of organic food. *International Journal of Consumer Studies*, 30(2), 155-163. <https://doi.org/10.1111/j.1470-6431.2005.00472.x>
- 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>
- Jaspers, E. D., & Pearson, E. (2022). Consumers' acceptance of domestic Internet-of-Things: The role of trust and privacy concerns. *Journal of Business Research*, 142, 255-265. <https://doi.org/10.1016/j.jbusres.2021.12.043>
- 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. *Advances in Consumer Research*, *11*,
- Karale, A. (2021). The challenge of IoT addressing security ethics, privacy and laws. *Internet of Things*, *15*. <https://doi.org/10.1016/j.iot.2021.100420>
- Kelley, P. G., Cranor, L. F., & Sadeh, N. (2013, April). 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>
- 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*. <https://doi.org/10.1016/j.cose.2019.101571>
- Lodge, T., Crabtree, A. (2019). Privacy engineering for domestic IoT: Enabling due diligence. *Sensors*, *19*(20). <https://doi.org/10.3390/s19204380>
- Nordgren, L. F., Van Harreveld, F., & Van Der Pligt, J. (2006). Ambivalence, discomfort, and motivated information processing. *Journal of experimental social psychology*, *42*(2), 252-258. <https://doi.org/10.1016/j.jesp.2005.04.004>
- Park, B., Park, S., & Billings, A. C. (2020). Separating perceptions of Kaepernick from perceptions of his protest: An analysis of athlete activism, endorsed brand, and media effects. *Communication & Sport*, *8*(4-5), 629-650. <https://doi.org/10.1177/2167479519894691>
- 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>
- Schuitema, G., Aravena, C., & Denny, E. (2020). The psychology of energy efficiency labels: Trust, involvement, and attitudes towards energy performance certificates in Ireland. *Energy Research & Social Science*, *59*. <https://doi.org/10.1016/j.erss.2019.101301>
- Shen, Y., & Vervier, P., A. (2019). IoT security and privacy labels. *Privacy Technologies and policy*, 136-147. [https://doi.org/10.1007/978-3-030-21752-5\\_9](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>
- Tabassum, M., Kosiński, T., & Lipford, H. R. (2019). “I don’t own the data”: End user perceptions of smart home device data practices and risks. *Proceedings of the 15th Symposium on Usable Privacy and Security, SOUPS 2019*.
- Tilburg University. (2019, June 21). *TILT participates in large project on Internet of Things dutch national research agenda*. Retrieved 2022, January 15 from <https://www.tilburguniversity.edu/current/miljoenenproject-internet-things>
- 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 attitudes, material access, skills, and usage, *Information, Communication & Society*, 24(2), 258-276. <https://doi.org/10.1080/1369118X.2019.1646777>
- van Strien, J., L., Kammerer, Y., Brand-Gruwel, S., & Boshuizen, H. P. (2016). How attitude strength biases information processing and evaluation on the web. *Computers in Human Behavior*, 60, 245-252. <https://doi.org/10.1016/j.chb.2016.02.057>

## **Appendix A**

### **Scenario**

In the next few pages, imagine that you are in a store and considering to buy a smart speaker. For context:

Using your voice, you can command smart speakers to do different things for you. You can set appointments, create shopping lists, set alarms, listen to music and ask all kinds of questions about the weather, the news, the current TV programme or math problems. If the smart speaker is connected to other devices in your house, you could also control the lights or temperature by voice command.

In the following pages, you will be shown smart speakers along with different security labels. The information is given by an independent organization using a standardized procedure to test the security of the device. Please look at the labels carefully and then answer the questions.

## **Appendix B**

### **Attitude Scale B1**

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

Boring – Exciting

Negative – Positive

A bad idea – A good idea

Unhelpful – Helpful



## Purchase Intention item B2

(1) Extremely unlikely – (7) Extremely likely

Under the assumption that you are looking for a smart speaker, how likely are you to purchase the smart speaker based on its description?"

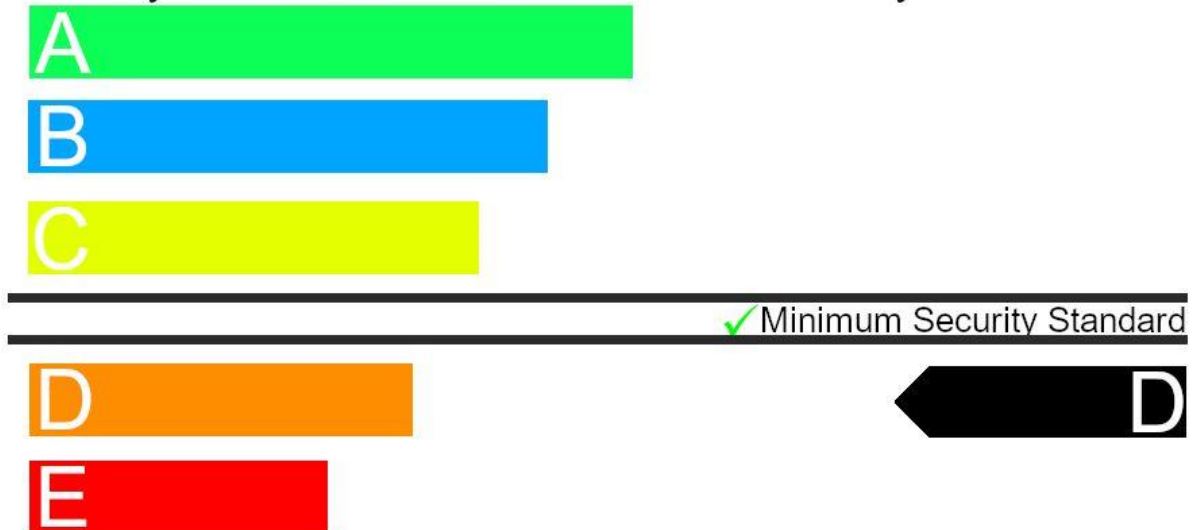
### Appendix C

#### Graded Labels

**Figure C1**

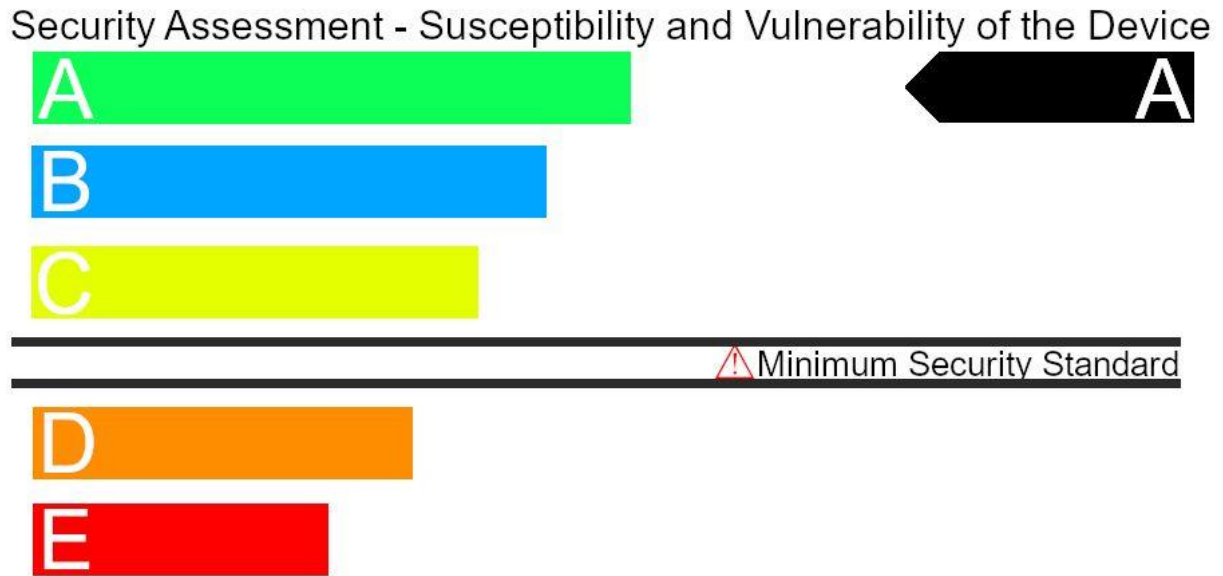
*Graded smart speaker label with low security degree and positive framing*

Security Assessment - Protection and Security of the Device



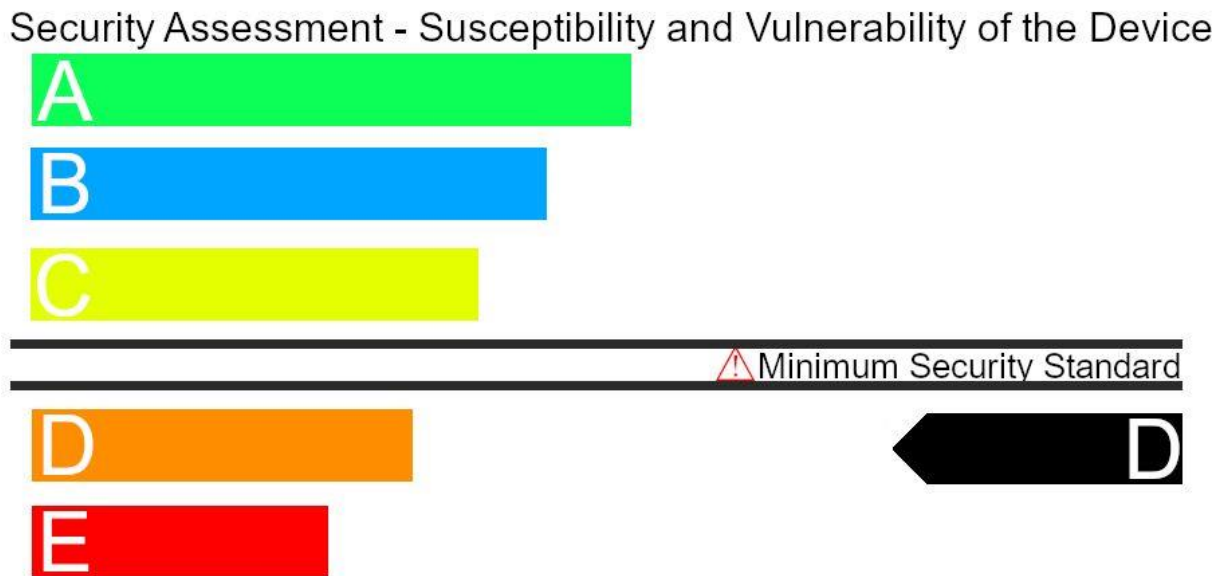
**Figure C2**

*Graded smart speaker label with high security degree and negative framing*



**Figure C3**

*Graded smart speaker label with low security degree and negative framing*




## Appendix D

### Informative Labels

**Figure D1**


*Informative smart speaker label with low security degree and positive framing*

<b>Security Assessment</b>		
Protection and Security of the Device		
<b>Security</b>  	Update*	Manual <span style="float: right;">✓</span>
	Password*	No
	Authentication*	No
	Encryption*	No
	Internet access	Yes
	Connect to other devices	Yes

\* required for minimum security standard

**Figure D2**


*Informative smart speaker label with high security degree and negative framing*

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

\* required for minimum security standard

**Figure D3**

*Informative smart speaker label with low security degree and negative framing*

<b>Security Assessment</b>		
Susceptibility and Vulnerability of the Device		
<b>Security</b>  	Update*	Manual
	Password*	No <span style="float: right;">!</span>
	Authentication*	No <span style="float: right;">!</span>
	Encryption*	No <span style="float: right;">!</span>
	Internet access	Yes
	Connect to other devices	Yes

\* required for minimum security standard

## Appendix E

### Questionnaire

You are invited to participate in this survey on smart devices. We are interested in your personal thoughts on smart devices, so there are no right or wrong answers. We will present you with some smart speakers and would like to know how willing you are to purchase them based on their descriptions. These descriptions are in the form of labels and vary in design.

This study will take around 5 to 15 minutes to complete, but you can take as much time as you want. Your information will be kept anonymous and confidential. No identifiable information will be saved or published and no one but the researchers have permission to view your data. This survey is completely voluntary, you can withdraw from it at any point in time. If you want your data removed you can contact the researcher.

If you have any concerns or questions you can contact: *m.k.walterscheid@student.utwente.nl*  
Do you consent to these terms and conditions?

- Yes
- No

What is your gender?

- Male
- Female
- Prefer not to say
- other (specify)

What is your age?

What is your country of origin?

What is the highest level of education that you have completed?

- Elementary school
- Highschool
- College
- Trade school
- Bachelor
- Master
- PhD

ID If you are here from the Sona-system, please enter your Identity code (**five numbers long, not your student number**), in order to receive credits for completing the survey.

Please tell us...

	Nothing at all	A little	A moderate amount	A lot	A great deal
How much do you know about smart speakers? (e.g. Alexa, Amazon Echo, Google Nest etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Please tell us what you think about using smart speakers in your own home in the future.  
Taking **security** into account, using a smart smart speaker device would be:

	1	2	3	4	5	6	7	
	1	2	3	4	5	6	7	
Foolish	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Wise
Worthless	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Valuable
Boring	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Exciting
Negative	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Positive
A bad idea	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	A good idea
Unhelpful	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Helpful

In the next few pages, imagine that you are in a store and considering to buy a smart speaker. Please read this information to understand the following scenario:

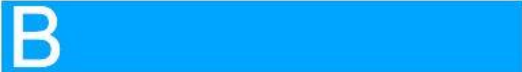
Using your voice you can command smart speakers to do different things for you. You can set appointments, create shopping lists, set alarms, listen to music and ask all kinds of questions about the weather, the news, the current TV programme or math problems. If the smart speaker is connected to other smart devices in your house, you could also control the lights or temperature by voice command.

In the following pages, you will be shown smart speakers along with different security labels. The information is given by an independent organization using a standardized procedure to test the security of the device. Please look at the labels carefully and then answer the questions.

Please take a close look at the label and indicate how likely you are to buy this smart speaker.



Security Assessment - Protection and Security of the Device



✓ Minimum Security Standard







Please take a close look at the label and indicate how likely you are to buy this smart speaker.



Security Assessment - Protection and Security of the Device

A

B

C

✓ Minimum Security Standard

D

◀ D

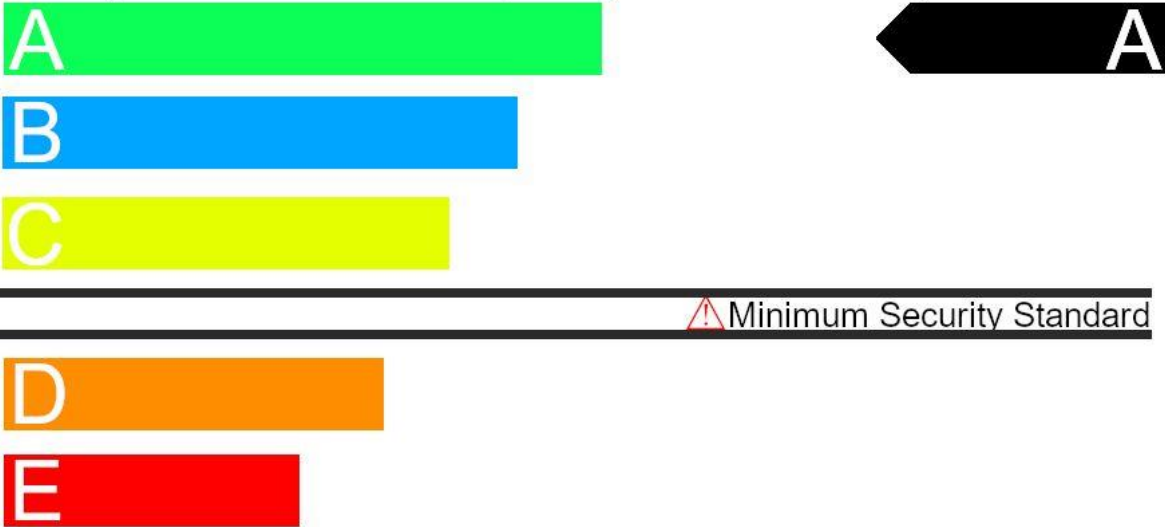
E



Please take a close look at the label and indicate how likely you are to buy this smart speaker.



Security Assessment - Susceptibility and Vulnerability of the Device

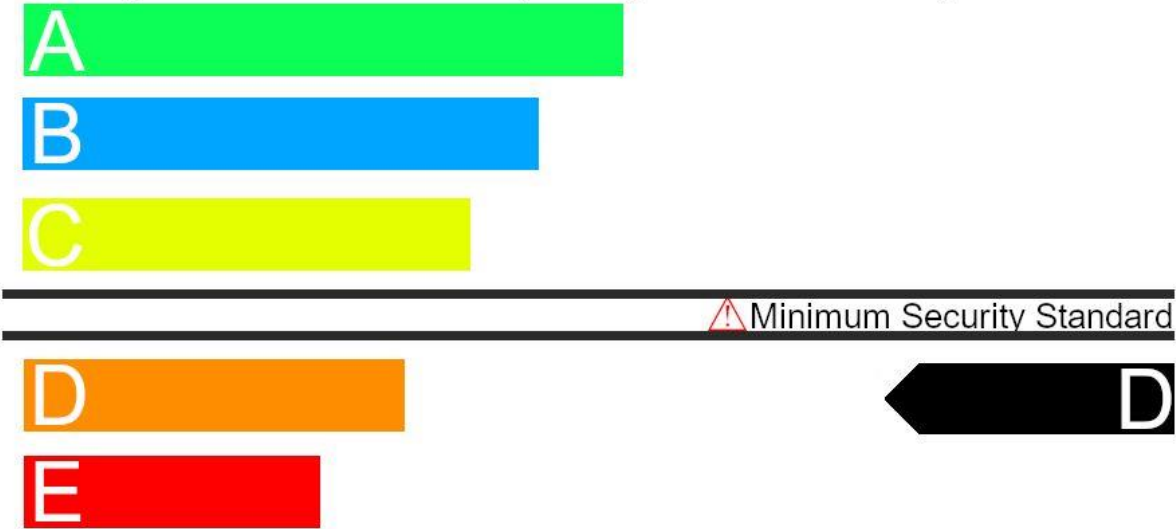




Please take a close look at the label and indicate how likely you are to buy this smart speaker.




Security Assessment - Susceptibility and Vulnerability of the Device





Please take a close look at the label and indicate how likely you are to buy this smart speaker.



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


\* required for minimum security standard





Please take a close look at the label and indicate how likely you are to buy this smart speaker.




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

\* required for minimum security standard



Please take a close look at the label and indicate how likely you are to buy this smart speaker.




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

\* required for minimum security standard



Please take a close look at the label and indicate how likely you are to buy this smart speaker.



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

\* required for minimum security standard

	Extremel y unlikely	Moderatel y unlikely	Slightl y unkelik y	Neither likely nor unkelik y	Slightl y likely	Moderatel y likely	Extremel y likely
How likely are you to purchase the smart speaker based on its description ?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
How likely do you think it is that the description presents correct information ?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Looking at the two label types:  
which type do you prefer?

- First one
- Second one
- I don't prefer one over the other

Can you tell us why? (voluntary)