

IoT labels' impact on security and privacy concerns

Yi-Shyuan Chiang

Siebel School of Computing & Data Science
University of Illinois Urbana-Champaign
Urbana, United States
ysc6@illinois.edu

Pardis Emami-Naeini*

Computer Science Department
Duke University
Durham, United States
pardis@cs.duke.edu

Camille Cobb*

Siebel School of Computing & Data Science
University of Illinois Urbana-Champaign
Urbana, United States
camillec@illinois.edu

Abstract—Countries are launching Internet of Things (IoT) cybersecurity label programs to help consumers make more informed purchasing decisions and motivate manufacturers to create more secure IoT products. In such programs, products that meet program requirements can be sold with a special label to signal cybersecurity compliance. Currently, there is no evidence-based guidance or standardized implementation of labels or label-awarding program policies. We conducted an online survey to understand the impact of IoT labels and choices such as validation requirements (i.e., whether manufacturers need to self attest or seek third-party audits to validate their products' compliance) regarding participants' security and privacy concerns. Our research provides empirical evidence to guide policy choices by effective label-awarding programs. We find that the presence of IoT labels alleviated both security and privacy concerns; however, we did not find differences between other program implementation choices. We provide recommendations for IoT cybersecurity label programs and discuss the potential societal impacts of label programs.

Index Terms—IoT, IoT label, label program design

I. INTRODUCTION

The prevalence of Internet of Things (IoT) devices has led to an increase in attacks that are IoT-specific [1]. Consumers of IoT devices are exposed to an unprecedented number of privacy and cybersecurity threats [2]. Privacy intrusion has been one of the most prevalent digital harms to consumers [3], such as unauthorized data collection, unauthorized access, and publication of sensitive information [4]–[6].

One way to enhance IoT device security would be to incentivize device manufacturers to adopt protective security and privacy practices. Recently, national governments have initiated *label-awarding programs* as incentives to establish baseline cybersecurity requirements [7] (Figure 1). In these label-awarding programs, governments award labels to devices that meet certain cybersecurity requirements. Manufacturers are allowed to display the labels on product packaging to indicate that the devices are more secure, as they have met the requirements. As of May 2025, there are three established label-awarding programs: Finland, Germany, and Singapore [7]–[9]. For example, Finland launched the first program in late 2019¹.

Previous work on IoT labels focused on the design aspects of the labels, such as how much information should be

* Denotes equal contribution.

¹Although the US program has been announced, the program has not accepted applications since its creation in May of 2025 [10].

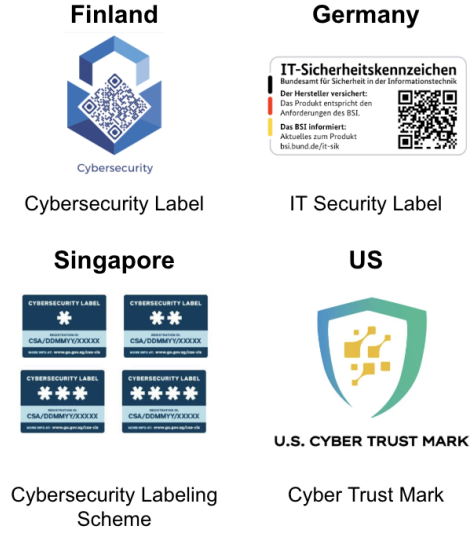


Fig. 1. Existing IoT cybersecurity labels.

presented on, and in what way [11]–[13]. Researchers have not studied the effects of different IoT label-awarding program designs as the recency of existing programs has precluded the availability of such empirical data for analysis. Label-awarding programs vary across different aspects, such as what standards devices need to abide by, how many levels of labels are there, and how the compliance has been validated (Figure 2).

This study focuses on two of these aspects: *label granularity* (whether there are multiple levels of labels manufacturers could apply for) and *validation requirements* (whether manufacturers can self attest that their products meet required standards or if they require third-party audits). Some existing programs award *binary* labels [8], [9] while others award *multi-level* labels [7]. Programs' validation requirements include *audit* [7], [8] and *self-attestation* [7], [9].

As IoT label-awarding programs are created, authorities must make decisions about how they are implemented, but these decisions are currently based on assumptions and beliefs rather than research-based understandings within this specific context of use [10]. It is crucial to understand whether and how various label awarding policies impact consumers' security and privacy concerns because these choices will determine programs' efficacy. For example, *multi-level labels* might

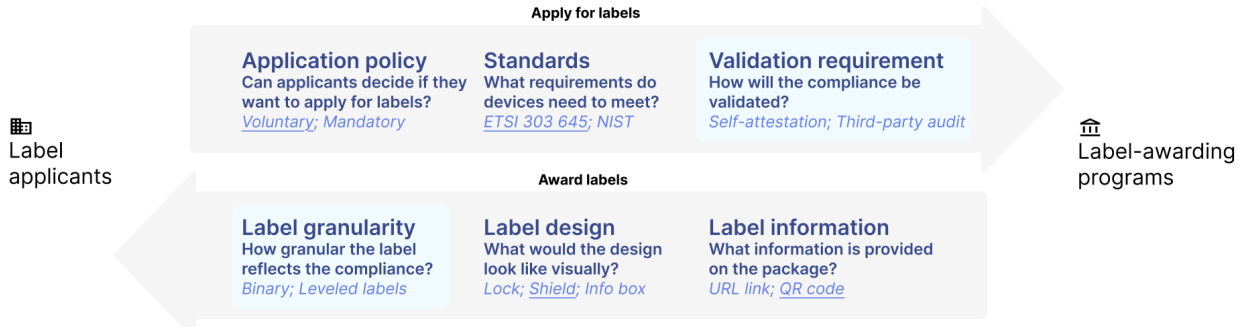


Fig. 2. **Aspects of label-awarding programs.** Validation process and label granularity, highlighted in pastel blue, are the two aspects we focused on in this study. Other aspects, such as the application policy, standards, label designs, and label information, are the same in the conditions used in this study.

introduce more confusion for consumers while providing more information; stricter *validation requirements* might discourage manufacturers' willingness to apply but increase consumers' security and privacy protection.

All existing programs are still relatively new; no research leverages the program designs laid out by existing real-world label-awarding programs. We ground this study with the signaling theory [14]. Signals are actions, attributes, or communication that signal the unobservable qualities to the external parties [15]. In a consumer-facing context, certification is one of the signals companies can send out to differentiate themselves from the competitors [15], [16]. For example, EnergyStar is an important signal for energy efficiency of appliances and homes [17], [18]. IoT labels can potentially signal compliance with cybersecurity requirements when the label-awarding programs are fully voluntary; however, we do not currently know how effective these IoT labels are as signals. To help guide the design of future IoT label-awarding programs and/or revisions to existing programs, we assume label-awarding programs are already in place and ask the following research questions:

- RQ1: To what extent do labels affect security and privacy concerns about IoT devices?
- RQ2: To what extent do other aspects of label program design (i.e. label granularity, validation requirement) affect users' security and privacy concerns about devices?
- RQ3: How do label program designs (i.e. label design, label information) impact how informative and easy-to-understand the labels are to users?

To address these research questions, we deployed an online survey. The survey consisted of an experimental component, in which participants reacted to one of seven label program descriptions which varied in terms of *label granularity* and *validation requirement*. Within the context of that program, an image of an IoT product either did or did not have a label on its package. Participants then reported on their information searching habits for IoT devices. The program descriptions and product images in this study take inspiration from existing label-awarding programs in Finland, Germany, and Singapore.

We recreated label-awarding programs as close to existing programs as possible. For example, we adopted the same set of cybersecurity guidelines used by Finland, Germany,

and Singapore [7]–[9]. We incorporated the logo and QR code combination design in our own visual design of the label (Finland, Germany) [8], [9]. We also referred to the Memoranda of Understanding (MoU) when mapping the levels between the binary label programs and the different levels from the leveled label program [7]. See Section II-C for more details.

We found that, regardless of the program description, participants had lower security and privacy concerns about products with a label than those without. However, we did not find a statistically significant difference between the effects of different aspects of label programs, such as label granularity or validation requirements. Over half of the participants reported that they found the label in our study at least somewhat informative and easy to understand, even though there was significantly less information on the label compared to IoT nutrition labels that have been proposed by researchers. We discuss our findings' implications about how label-awarding programs should be designed and how existing programs stand in the context of our recommendations.

II. BACKGROUND AND RELATED WORK

In this section, we discuss previous work on privacy and security nutrition labels. We introduce the existing IoT cybersecurity guidelines and IoT label-awarding programs.

A. Privacy and security nutrition labels

Labels are easy-to-understand visual components often used to convey important information about products. Labels are found in contexts like food packaging, medical devices, and household appliances (i.e., ENERGY STAR labels) [17], [19], [20]. Kelley et al. were the first to propose labels – styled similarly to food nutrition labels – in the context of web privacy in 2019 [21]. Proposed privacy nutrition labels allowed the readers to find standardized information faster and enhanced the enjoyment of reading content about web policies [21], [22].

Privacy nutrition labels are now available for mobile apps. Google introduced Data Safety Sections (DSS) that summarize what data apps collect [23]. In 2023, Apple announced the Privacy Nutrition Labels and App Privacy Report for apps [24]. Research on the efficacy and usability of these app privacy labels is still ongoing [25]–[28]. It is not yet clear whether

app labels are successfully pushing developers toward more secure practices.

As users grow increasingly concerned about IoT security but struggle to evaluate specific risks [29]–[32], researchers have expanded privacy nutrition labels to IoT. Studies have explored what information should be included on these labels, for example, based on experts’ perspectives [11]. Researchers have proposed different IoT nutrition labels and online systems with real-time product comparison [33]–[35]. For example, Emami-Naeini et al. proposed a multi-layered label design where the package contains only essential information and details are accessible via QR codes [12]. Recently, focuses have shifted toward the perception and impacts of specific designs, e.g., different visual designs, different information complexity [13], [36]. Participants are found to prefer designs with more information than the common minimalist designs [13]. QR code designs experience usability issues as people are reluctant to scan for different reasons, such as inconvenience and distrust in QR codes [13].

The labels awarded by IoT labeling-programs are more similar to “seal of approval” such as the US ENERGY STAR labels or Non-GMO labels than nutrition labels, as the labels have minimalist designs and bear limited information. Label programs might create a confusing ecosystem of varying certification organizations and fake or misleading labels [37], [38]. Moreover, there have been problems with the laboratories designated as testing and certification bodies. For example, the US Government Accountability Office (GAO) reported in 2010 that they were able to obtain ENERGY STAR certifications for fake products, including a “gas-powered alarm clock” [39].

B. IoT cybersecurity guidelines

In response to surging IoT attacks, governments have started providing best practice guidelines and launching programs to incentivize manufacturers to provide stronger infrastructure. These regulatory efforts can be categorized into IoT cybersecurity guidelines and IoT label-awarding programs [40]. IoT cybersecurity guidelines, one of the regulatory efforts, lay out basic standards that IoT devices should meet. The United Kingdom released the first IoT security guidelines, *Code of Practice for Consumer IoT Security*, in 2018 [41]. The European Telecommunications Standards Institute (ETSI) published two cybersecurity-related documents, *Cyber Security for Consumer Internet of Things (ETSI EN 103 645)* in 2019 and *Cyber Security for Consumer Internet of Things: Baseline Requirements (ETSI EN 303 645)* in 2020 [42], [43]. The former contains 13 cybersecurity provisions while the latter translates the provisions into concrete requirements. We refer to these as “ETSI baselines” throughout this paper. ETSI baselines are the most widely adopted guidelines [44]. We discuss programs and their awarding policies below.

C. Established IoT label-awarding programs

IoT label-awarding programs award products with IoT labels – visual representations of compliance with cybersecurity requirements. There are currently established programs in

Finland, Singapore, and Germany (Figure 1). Though the US announced the Cyber Trust Mark program in March 2024, it is unavailable for application in 2025. Therefore, the US program will not be in the scope of discussion for this study.

All existing programs are voluntary; manufacturers can decide to apply for labels but are not required to have labels to sell their products. All three countries use the ETSI baselines as requirements, but differ in terms of their label granularity (binary vs. leveled labels) and validation requirements (third-party audit vs. self-attestation).

1) *Label granularity*: Images of labels from Finland, Germany, and Singapore are shown in Figure 1. Finland and Germany both use binary labels, which are essentially seals of approval; all products that meet program requirements can use the same label [45]. Singapore’s *Cybersecurity Labeling Scheme* has four levels of labels [7], [46]. All levels share the same label design except stars indicating the label’s levels. Manufacturers decide which level to apply for. Level 1 requires products to meet the three most basic provisions of ETSI baselines (i.e., is the least restrictive and offers minimal guarantees to consumers). Levels 2, 3, and 4 require fulfillment of all 13 ETSI baselines and differ in terms of validation requirements.

2) *Validation requirements*: The biggest difference between Finnish and German programs is in the validation requirement, e.g., whether third-party audits are required. To earn a Finnish *Cybersecurity Label*, manufacturers must submit self-assessment forms to the Finnish Transport and Communications Agency, receive approvals, and get audits from independent laboratories. For the German *IT security label*, manufacturers apply by mailing the application form with self-attested evidence to the Federal Office for Information Security, which awards labels after reviewing materials. Singapore’s Level 1 and 2 labels both require only self-attestation, whereas Levels 3 and 4 require additional tests from independent laboratories (binary tests for Level 3 and penetration tests for Level 4).

3) *Mutual recognition between programs*: To work toward international collaboration, some countries have signed MoUs, indicating mutual recognition of each other’s programs. Singapore has MoUs with both Finland and Germany [7]. Under the current MoUs, German labels are recognized as Level 2 Singaporean labels and Finnish labels would be seen as the equivalent of Level 3.

III. METHODS

We conducted an online survey with US participants to address the research questions in the early summer of 2023. We studied the signaling effects of labels and aspects of label-awarding programs (i.e., label granularity, validation requirement) on security and privacy concerns (see Table II). We also inquired about the level of informativeness and understandability of the labels.

A. Recruitment and demographics

We conducted our survey on the Prolific crowdsourcing platform and collected 179 valid responses. All participants

Age	18-24 (33), 25-34 (70), 35-44 (32), 45-54 (21), 55-64 (17), 65 and above (9)
Gender	Female (82), Male (94), Non-binary (6)
Education	Less than a high school diploma(3), High school degree or equivalent (57), Associate degree (19), Bachelor's degree (70), Master's degree (24), Professional degree (5), Doctorate (3), Prefer not to answer (1)
Income level	Less than \$10,000 (8), \$10,000-\$19,999 (13), \$20,000-\$29,999 (19), \$30,000-\$39,999 (14), \$40,000-\$49,999 (13), \$50,000-\$59,999 (20), \$60,000-\$69,999 (13), \$70,000-\$79,999 (10), \$80,000-\$89,999 (20), \$90,000-\$99,999 (9), \$100,000-\$ 149,999 (21), \$150,000 or more (20), Prefer not to answer (2)
Device ownership	I do not own any device (20), I own one or more devices (162)
In market status	I am not in the market to buy any smart device (92), I am in the market for at least one devices (90)

TABLE I
PARTICIPANT DEMOGRAPHICS AND IoT BACKGROUND. THE NUMBER OF PARTICIPANTS WITH EACH DEMOGRAPHIC CHARACTERISTIC IS IN PARENTHESES.

were 18 years or older and consented to participate in the study. The median completion time was 4.5 minutes, and participants received USD \$1.23. This is roughly equivalent to USD \$17/hour (well above US federal minimum wage).

90% of participants owned one or more smart devices, which is slightly higher than Statista consumer insights' finding of an 85% smart home adoption rate [47]. Half of the participants were considering buying a(nother) device, which is comparable to a previously reported 70% of homeowners [48].

This work was supported by Consumer Reports (CR) and conducted by the first author during her time as a CR Fellow in Summer 2024. CR did not have an internal review board for this survey; however, the survey has been reviewed and approved by relevant internal departments to ensure that we did not collect identifiable information and that the study bore no risk or minimal risk to participants.

B. Label-awarding program designs

Each participant was randomly assigned to read and react to one out of seven label conditions. Each condition contains a short description and an image of a device (see Figure 3). The seven label conditions are from three programs based on the existing label-awarding programs: Program 1 (Germany-inspired), Program 2 (Finland-inspired), and Program 3 (Singapore-inspired). Conditions varied along two axes: label granularity (whether the program offers binary or leveled labels) and validation requirement (whether products need to pass third-party audits). Binary programs (Programs 1 and 2 in Figure 3) award only one level of label – products can either have a label or not. Leveled programs (Program 3 in Figure 3) award two or more levels of labels depending on what standards or validation requirements a product meets; in our study, there are just two levels. Our leveled program and wording mirrors the existing one in Singapore also in terms of its validation requirements: all labeled products are expected to adhere to the *same* set of standards, but products can earn a Level 2 label only if manufacturers obtain third-

party audits, whereas they can earn a Level 1 label with only self-attestation.

C. Survey process

We experimentally varied the label-awarding program description and product image to understand the effects of label presence (RQ1) and other aspects of label program design (i.e., label granularity, validation requirement) (RQ2). We also asked participants to rate the informative and easy-to-understand level of the label available in the label program they were shown (RQ3). We include the survey instrument in Appendix A, showing the question phrasing and flow for one of the seven conditions.

The first section of the survey focused on eliciting participants' attitudes and concerns toward the label design and its requirements. To ensure all participants had a baseline understanding of the IoT label, we gave a brief introduction:

To increase the security and privacy transparency of smart home devices, the government launched a **voluntary** labeling system. Manufacturers are encouraged to apply when they have met the security requirements, such as ensuring the software integrity and data safety.

We then presented each participant with one of three descriptions of specific label-awarding programs. Each description included the program's validation requirement and label granularity (see Table II). The following example describes a program with a binary label granularity and third-party audit validation requirement:

The manufacturers will be awarded the label once the product has passed third-party audits conducted by labs approved by the government. The products need to meet all requirements to pass the audits.

Since all existing programs have a voluntary application policy, we kept this program detail consistent for all participants and included it in our introduction to the concept of IoT label-awarding programs (see above). Programs' standards required to obtain a label were also described the same way for all participants and were chosen to reflect global norms (i.e., using ETSI EN 303 645 as the standard).

We also showed each participant all of the labels that could exist under the program described to them. We used a consistent label design (a shield) and label information (a QR code which was non-functional for this study to avoid introducing confounds if some participants used it to seek more information). The shield shape in our design was inspired by Australia's Stay Smart Reports [49], and the inclusion of a QR code echoed the common designs from existing label-awarding programs [7]–[9]. If the program described a binary label granularity, there was only one label (pictured below).














Label level Label program	No label	Level 1 label	Level 2 label
Program 1 Germany-inspired Voluntary Binary Self-attestation	Condition 1 (N = 27) 	Condition 2 (N = 24)   	n/a
Program 2 Finland-inspired Voluntary Binary Third-party audit	Condition 3 (N = 25) 	Condition 4 (N = 26)   	n/a
Program 3 Singapore-inspired Voluntary Mixed validation requirement	Condition 5 (N = 25) 	Condition 6 (N = 26)   	Condition 7 (N = 26)   

Fig. 3. The seven conditions we varied in terms of label presence and label-awarding programs. The yellow circles highlight the placement of the labels on the packages. The ones participants read did not have yellow circles; however, participants were reminded about whether products are awarded with labels in text.

Label presence	0 for no label. 1 for with label.
Label granularity	0 for binary labels. 1 for leveled labels.
Validation requirement	0 for manufacturer self-attestation (no third-party audit). 1 for third-party audit.

TABLE II

DEPENDENT VARIABLES OF THE CLMS LABEL PRESENCE, LABEL GRANULARITY, AND VALIDATION REQUIREMENT ARE THE THREE FACTORS THAT WE VARIED IN THE SETTINGS AND THE CLMS.



We then showed each participant an image of an IoT product in its packaging (such as the one below). All participants were shown the same product – a smart speaker in relatively plain packaging attributed to a fictional manufacturer. Because the label was relatively small in the image, we called attention to it in writing. For example, the text corresponding to the image below would read: “When looking at the package, you realize that this product *does* have an IoT label.”



After engaging with the aforementioned content, participants answered the following questions:

- How concerned are you about the security protection of the product? (1 Not concerned to 5 Concerned)
- How concerned are you about the privacy aspects of the product? (1 Not concerned to 5 Concerned)
- How easy or difficult is it for you to understand the label? (1 Easy to 5 Difficult)
- How informative do you think this label is to you? (1 Informative to 5 Not informative)

D. Data analysis

For concern levels collected in the first part of our survey, we built two cumulative link models (CLM) with `clm` from the `ordinal` packages in R. We quantified the effects of our experimental manipulations on how much security and privacy concerns the participants reported having about the product in the image shown to them. One model addressed the dependent variables of security concern, and the other addressed privacy concern; both shared the same set of independent variables: label presence, label granularity, and validation requirement (see Table II). We ran an a priori sample test with G*power linear regression settings [50], as CLMs have not yet had a conventional sample size test (73, 10 participants per condition). Within our budget, we recruited 2.6x of the same size results (182, 26 per condition). After data cleaning, we had 179 valid answers. For the analysis of informativeness and understandability, we conducted Kruskal-Wallis tests and post hoc Dunn tests using the `dplyr` package in R to examine whether there is a significant difference between the levels of

informativeness and understandability. We used the package built in Bonferroni correction for the post hoc Dunn’s tests.

E. Limitations

These data points are self-reported, which has limitations. Self-reported assessments have been reported to be highly correlated with actual behaviors [51]–[53]; the effects might still not fully reflect reality. Informativeness and understandability levels may be lower. We did not include comprehension checks to confirm participants’ understanding of the label-awarding programs. We should interpret these results as a high estimate of informativeness and understandability. Existing programs include the objectives, to improve security and privacy, in public announcements and news. We acknowledge that our online survey might have limited ecological validity in terms of its ability to mirror real-life shopping experiences; we created mock-up products that, to our ability, best resemble real products and existing IoT label designs. The mock-up products we created resemble real products, but the absence of brand names might impact findings; brand trust and loyalty are known to impact consumers’ purchase decisions [54], [55]. The QR code included would not direct the participants to an online portal since we wanted to limit the confounding factors we introduced. This might lower the overall informative level as not all information is provided. Minimal on-package information was part of the efforts to make the presentation as realistic as existing programs. Compared to prior research, the information on our package was very minimal. The limited amount of information could also affect the overall informativeness level.

IV. RESULTS

We found that labels did indeed lower security and privacy concerns (RQ1); however, we did not find measurable differences between different label programs (neither label granularity nor validation requirement) (RQ2). We found that participants found the common label design, the combination of a label and a QR code, to be at least somewhat informative and not hard to understand (RQ3).

A. Do labels affect S&P concerns? (RQ1)

To answer RQ1 and RQ2, we explore whether participants rated their security and/or privacy concern levels about an IoT product differently in our seven experimental conditions. Participants provided their security and privacy concern levels for the one-label program condition they saw. We used CLMs to assess whether the presence of labels, label granularity, and validation requirements affected security and privacy concerns.

Participants had lower security and privacy concerns about smart devices with labels than without. As shown in Figure 4, participants tended to report lower concern levels when we showed them *had* an IoT label. When products did not have a label, over 75% of participants rated themselves as concerned or somewhat concerned about both security and privacy, whereas fewer than 45% were concerned or very concerned about products pictured *with* a label. To statistically

Coefficients:			
	Estimate	Std. Error	Pr(> z)
Label presence (baseline = No Label)			
With label	-1.40	0.30	***
Label granularity (baseline = Binary Label)			
Leveled label	0.37	0.29	
Audit requirement (baseline = No audit)			
Third-party audit	-0.04	0.29	

TABLE III

SECURITY CONCERN CLM. A NEGATIVE ESTIMATE INDICATES COMPARED TO THE BASELINE OF THE VARIABLES (FOR EXAMPLE, NO LABEL IS THE BASELINE) THE SPECIFIC LEVEL OF THE FACTOR (E.G., WITH LABEL) WOULD DECREASE THE REPORTED LEVEL OF CONCERN. A POSITIVE ESTIMATE SIGNALS THE OPPOSITE OF THE TREND.

Coefficients:			
	Estimate	Std. Error	Pr(> z)
Label presence (baseline = No Label)			
With label	-1.37	0.30	***
Label granularity (baseline = Binary Label)			
Leveled label	0.39	0.29	
Audit requirement (baseline = No audit)			
Third-party audit	-0.13	0.29	

TABLE IV

PRIVACY CONCERN CLM. A NEGATIVE ESTIMATE INDICATES COMPARED TO THE BASELINE OF THE VARIABLES (FOR EXAMPLE, NO LABEL IS THE BASELINE) THE SPECIFIC LEVEL OF THE FACTOR (E.G., WITH LABEL) WOULD DECREASE THE REPORTED LEVEL OF CONCERN.

validate the above observation, we fit two CLMs, one with security concern levels and the other with privacy concern levels as the dependent variable. For both models, whether the product was shown with a label is represented by the label presence variable in the model: 0 meant No label and 1 meant With label. Results of our CLMs are shown in Table III and Table IV. We found that the presence of the label significantly reduced participants’ security concerns (*Est. coeff.* = -1.40 , $p < 0.05$) and privacy concerns (*Est. coeff.* = -1.37 , $p < 0.05$).

B. Do label granularity and validation requirement affect S&P concerns? (RQ2)

In addition to the overall pattern described above, which shows that the presence of a label results in lower security and privacy concerns, RQ1 also pushes us to consider whether other label program details impact concern levels. Specifically, the survey conditions varied in how they described the program’s *validation requirements* and *label granularity* (i.e., binary, in which products either have a label or not vs. leveled, in which products could have one of two labels or no label). The two CLMs described above include variables related to validation requirements and label granularity, and so they enable us to address RQ2 (Table IV, Table III).

We found no measurable effects of label granularity and validation requirements.

- *Label granularity:* We did not find any significant differences between the two levels of label granularity ($p > 0.05$). To further investigate whether there is a difference between the two levels in the leveled program,

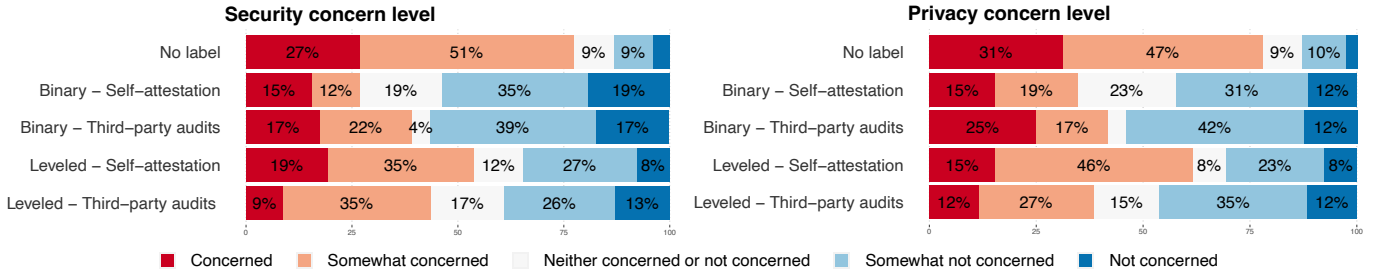


Fig. 4. **Distribution of participants' security and privacy concerns split based on whether they saw a label and – if so – the policies of the program that had been described to them.** No label conditions are Condition 1, 3, and 5. With binary labels are Condition 2 (Self-attestation) and 4 (Third-party audit); Leveled label with self-attestation is Condition 6 and Leveled label program with third-party audit is Condition 7 from Figure 3.

we performed Kruskal-Wallis tests for both security and privacy concerns. The results of the Kruskal-Wallis tests were also insignificant ($p > 0.05$).

- *Validation requirement:* We hypothesized that third party audits would be associated with lower security and privacy concerns; however, we did not find any significant differences between the two levels of validation requirement, self attestation v. third-party audit, either ($p > 0.05$).

We discuss some potential reasons for the lack of significant effects in validation requirements in Section V-B.

C. Are common label designs informative and easy to understand? (RQ3)

Compared to prior research, the common IoT label designs contain very little information. The designs usually contain a label and a QR code, without any specific details about the devices or the data type. We asked about perceptions of the common label design, a combination of a label and a QR code. The designs can be found in Figure 3.

Most participants found labels at least somewhat easy to understand (Figure 5). 65% of participants found labels to be at least somewhat easy to understand. Over one in ten participants found the labels (somewhat) difficult to understand (18%). We found that not all conditions are as easy to understand. There was a difference among all conditions between the understandability levels in a Kruskal-Wallis test ($p < 0.05$). Following up with post-hoc Dunn's tests, we found that the significant difference lay in Level 1 and Level 2 from the leveled program. These two conditions shared the same program introduction for the same leveled program; however, participants who saw Level 2 labels (*Median* = 2.5) found it harder to understand than those who read Level 1 labels (*Median* = 2).

Most participants found labels somewhat informative (Figure 6). 70% of participants reported the labels to be at least somewhat informative (*Somewhat informative* (43%), *Informative* (27%)). Conditions did not affect how participants perceived how informative the label was. There is no statistically significant result from a Kruskal-Wallis test among all seven conditions ($p > 0.05$). This means that regardless of the conditions participants were assigned to, they found the label to be similarly informative.

V. DISCUSSION

We provide recommendations for label-awarding programs and comments contextualized in existing label-awarding programs. We discuss the potential reasons, and how those would inform the design of future work that could make even more actionable recommendations.

A. Recommendations for label-awarding programs

We provide recommendations regarding ways to measure the signaling effects, program designs, and label design.

Measuring effectiveness of label-awarding programs. A key goal of our work was to provide recommendations for designing effective IoT label-awarding programs. Grounded in the signaling theory, effectiveness of programs could be measured by the privacy and security concern level changes because effective labels should signal the security and privacy attributes and lead to behavioral changes. However, in part due to the multi-stakeholder nature of label-awarding programs, such recommendations are not straightforward.

Signal effectiveness relies on program administrators, auditors, and/or device manufacturers to ensure program compliance and information accuracy. Signals are only effective when they are accurate and reliable. Effectiveness also depends on perceptions and purchasing decisions of consumers who have varying degrees of technology literacy and place differing amounts of weight on the importance of security and privacy. Regarding impact on purchasing decisions, Caven *et al.* found that the US Cyber Trust Mark labels did not affect the final purchasing decisions except for participants who already had some background in cybersecurity [56]. They did not give empirical insights about *why* purchasing decisions were not impacted by security and privacy concerns.

However, a perhaps more important metric of efficacy is whether programs help **reduce security and privacy harms** to consumers. If consumers are less concerned about security and privacy but devices do not actually meet appropriate standards, then programs could increase consumer harm rather than decrease it. As discussed in Section II, similar programs in other application domains have faced challenging situations in which devices did not meet the standards but still received labels: (1) Devices were erroneously certified. This could be caused by failed self-attestation or leniency of third-party auditors [39]. Erroneous certification could undermine the

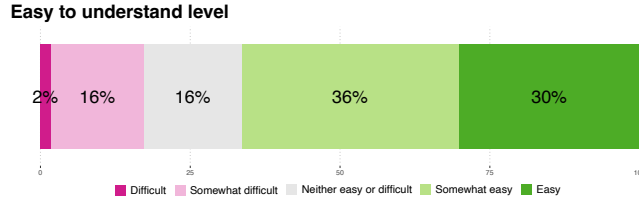


Fig. 5. **Distribution of easy-to-understand levels of the label.** Around two-thirds of the participants (66%) found our label design to be at least somewhat easy to understand.

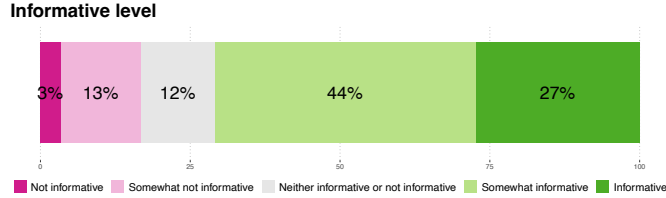


Fig. 6. **Distribution of informativeness levels of the label.** Over 70% of the participants found our label design to be at least somewhat informative.

overall credibility of labels and the signaling effects. (2) Devices were “labeled” with non-restricted images that were highly-similar to authentic, authorized labels [38]. Inauthentic labels might not directly discredit the signaling effects of legitimate labels; however, they might indirectly lower the signaling ability by creating more noise in the information searching processes where signaling usually takes place. We provide the following comments and recommendations for program design and label design with these situations in consideration.

Validation requirements. If stronger validation requirements (i.e. audits compared to self-attestation) are not interpreted as such by consumers (e.g., do not cause them to be *less* concerned about security and privacy), then it is clear that, all other factors being the same, stricter validation requirements should be preferred. We find that labels do decrease security and privacy concerns; however, there is no difference between labels with different validation requirements. We, therefore, recommend label-awarding programs to have stricter validation requirements, such as third-party audits.

Label granularity. If participants provide similar concern levels for different leveled labels, this means that the intended label granularity has not been interpreted by the participants. Besides finding no evidence for the difference between labels of different levels, we also find that leveled labels might be more difficult to understand. Our results echo previous work that has shown that the complexity of leveled labels can be less effective at affecting purchasing decisions, which might be due to the complexity of the label-awarding system [45]. We recommend more research on leveled labels, such as how people interpret level programs and how to effectively communicate the program designs.

Visual design of labels The label designs from existing programs are all combinations of QR codes and a logo without additional information. Compared to previous usable security

and privacy literature, the labels in use are very minimalist. Most participants found labels in our study (somewhat) easy to understand (66%). While this may seem relatively high, we should ask if more than 30% not understanding is acceptable – especially because these ratings may be inflated due to acquiescence bias in self-reports. Label-awarding programs should refer to and support the ongoing usable security and privacy studies on IoT label designs [13], [36].

B. Reasoning the lack of effects from third party audits

One might hypothesize that labels requiring stricter validation (i.e., third party audits vs. self-attestation) would result in more significant reductions to participants’ security and privacy concerns. Our study design provided two chances to inquire about such a hypothesis: First, when participants see a labeled product, are their average concern levels lower if we had described Program 2 to them (which requires third-party audits) compared to if we had described Program 1 to them (self-attestation)? Second, when they are shown a description of Program 3, are concern levels lower for products with Level 2 labels (which require third-party audit) than for products with Level 1 labels (which require only self-attestation)? Surprisingly, in both cases, our data did not provide sufficient evidence to conclude that any difference exists. That is, participants’ concern levels for programs with third-party audits were similar to their concern level for programs with self-attestation (Section IV-B).

Why? One potential explanation is that participants do not (have enough information to) understand these differences, or they do understand but do not care about these differences in validation requirements. Another explanation for the lack of effects is that the program descriptions in our study did not specify *who* the third-party auditors were. We did not specify whether audits could only be conducted by third-party organizations that receive approval. Previous work found that participants wanted to know more about auditors’ identities

and what information is available to auditors for their decision-making [12]. We need to locate the real reason(s) behind this finding, as it would affect the future efforts of label-awarding programs. If the problem lies in technology literacy, then more research on information presentation and literacy enhancement is needed. If it were due to the lack of information about devices or the validation process, we will need more research on users' understandings of and preferences for the validation requirements and process.

C. Existing programs in the context of our recommendations

We recommended above that label-awarding programs require third-party audits. Finland's programs align with the recommendations. The highest two levels in Singapore's program (Level 3 and 4) also meet the recommendation. Germany's label and the lowest two levels of Singapore program are against our recommendation as they do not require third-party audits. To account for the credibility of label-awarding programs, it is important to ensure the quality of the products meets the validation requirements. Some label-awarding programs have made efforts to ensure the label programs and audits remain credible. Finland's program reviews labeled devices every two years; products that fail or do not undergo reviews lose the right to use the label [57]. Products using the German label can be subject to a compliance test at any time, which is done on a random or ad hoc basis [58]. The random compliance test component is more in line with our recommended third-party audits.

We recommend more research on leveled programs, such as how people understand leveled labels and how label-awarding programs can assist people to make decisions. Singapore's program is the only leveled program. It has four levels of labels, two more than the programs we've shown in this study. Our study suggests that leveled programs may introduce confusion without additional information to help consumers differentiate between the different levels. Label-awarding programs should refer to the existing literature on effective IoT label designs and presentation.

D. An agenda for label-awarding programs designs

Past research focuses on studying the transparency aspects of IoT labels, i.e., how much product information should be on the package? What visual designs are the most effective in conveying the information? Studies on people's preferences for product-specific information presentation have saturated: people prefer more information in an easily accessible manner have gradually been confirmed. Shifting away from product-specific information presentation, we focus on the underlying designs of the label-awarding programs in this study. Moving forward, here are 3 questions for program stakeholders to reflect on when designing or revising the programs:

- 1) What are the desired effects of the label-awarding program? We've found that labels are effective at signaling security and privacy properties, as evident by the lowered concern levels. Programs might have other

objectives they aim to target, such as enhanced trust or transparency.

- 2) What are the validation requirements of the label-awarding program? We did not find evidence to support the difference between validation requirements; however, this does not mean there are no real differences for real label-awarding programs. Program stakeholders should carefully consider the implications of validation requirements and conduct more research if needed.
- 3) What level of transparency does the label-awarding program aspire to have? We found that the participants found our label with minimal information to be at least somewhat informative. Program stakeholders need to decide whether they are comfortable with providing the bare minimum or incorporating more information in a layered fashion as suggested in previous work.

VI. CONCLUSION

In this study, we conducted an online experiment to understand the effects of the presence of IoT labels and different aspects of label-awarding programs. We found that the presence of labels alleviate privacy and security concerns. Participants report lower concern levels when they see products with labels. Despite the differences in awarding policies, the different awarding policies have similar effects concern levels. We discussed the potential societal impacts of IoT label-awarding programs and provided actionable recommendations for future program owners.

ACKNOWLEDGMENT

We thank fellow members of the CROPS lab and Dr. Lorrie Cranor for helpful feedback at various stages of the work. We thank Dr. Weijia He for guiding us through the shepherding process. We thank Consumer Reports for supporting this study through the 2023 CR Fellowship program.

REFERENCES

- [1] D. Jones, "DDoS attacks, growing more sophisticated, surged in Q2," <https://www.cybersecuritydive.com/news/ddos-attacks-surge/688464/>, 2023.
- [2] Y. Omer and P. Jorge, "DDoS threat report for 2023 Q2," <https://blog.cloudflare.com/ddos-threat-report-2023-q2/>, 2023.
- [3] D. Buil-Gil, S. Kemp, S. Kuenzel, L. Coventry, S. Zakhary, D. Tilley, and J. Nicholson, "The digital harms of smart home devices: A systematic literature review," *Computers in Human Behavior*, vol. 145, p. 107770, 2023.
- [4] M. Renda, "Company accused of spying on customers via sex toys," <https://www.courthousenews.com/company-accused-of-spying-on-customers-via-sex-toys/>, 2018.
- [5] S. Alkhatib, J. Waycott, and G. Buchanan, "Privacy in aged care monitoring devices (ACMD): The developers' perspective," in *Digital Health: Changing the Way Healthcare is Conceptualised and Delivered*. IOS Press, 2019, pp. 7–12.
- [6] L. H. Newman, "Millions of web camera and baby monitor feeds are exposed," <https://www.wired.com/story/kalay-iot-bug-video-feeds/>, 2021.
- [7] Cyber Security Agency of Singapore (CSA), "Cybersecurity labelling scheme (CLS)," <https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme>, 2020.
- [8] Finnish Transport and Communications Agency (Traficom), "Cybersecurity label," <https://tietoturvamerkki.fi/en/apply-label>, 2019.

- [9] Federal Office for Information Security, "IT security label," https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/IT-Sicherheitskennzeichen/fuer-Hersteller/Antrag/IT-SiK-Antrag_node.htm, 2021.
- [10] Federal Communications Commission, "In the matter of cybersecurity labeling for Internet of Things (PS Docket No. 23-239)," <https://docs.fcc.gov/public/attachments/FCC-24-26A1.pdf>, March 2024.
- [11] P. Emami-Naeini, Y. Agarwal, L. F. Cranor, and H. Hibshi, "Ask the experts: What should be on an IoT privacy and security label?" in *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2020, pp. 447–464.
- [12] P. Emami-Naeini, J. Dheenadhayalan, Y. Agarwal, and L. F. Cranor, "An informative security and privacy "nutrition" label for Internet of Things devices," *IEEE Security & Privacy*, vol. 20, no. 2, pp. 31–39, 2021.
- [13] C. C. Chen, D. Shu, H. Ravishankar, X. Li, Y. Agarwal, and L. F. Cranor, "Is a Trustmark and QR code enough? The effect of IoT security and privacy label information complexity on consumer comprehension and behavior," in *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, 2024, pp. 1–32.
- [14] M. Spence, "Job market signaling," in *Uncertainty in economics*. Elsevier, 1978, pp. 281–306.
- [15] B. L. Connelly, S. T. Certo, C. R. Reutzel, M. R. DesJardine, and Y. S. Zhou, "Signaling theory: State of the theory and its future," *Journal of management*, vol. 51, no. 1, pp. 24–61, 2025.
- [16] A. A. King, M. J. Lenox, and A. Terlaak, "The strategic use of decentralized institutions: Exploring certification with the ISO 14001 management standard," *Academy of management journal*, vol. 48, no. 6, pp. 1091–1106, 2005.
- [17] ENERGY STAR, "How a product earns the Energy Star label," <https://www.energystar.gov/products/how-product-earns-energy-star-label>, 2023.
- [18] R. B. Paton, "Two pathways to energy efficiency: An Energy Star case study," *Human Ecology Review*, pp. 247–259, 2004.
- [19] U.S. Food and Drug Administration, "How to understand and use the nutrition facts label," <https://www.fda.gov/food/new-nutrition-facts-label/how-understand-and-use-nutrition-facts-label>, 2022.
- [20] —, "Device labeling," <https://www.fda.gov/medical-devices/overview-device-regulation/device-labeling>, 2020.
- [21] P. G. Kelley, J. Bresee, L. F. Cranor, and R. W. Reeder, "A "nutrition label" for privacy," in *Proceedings of the 5th Symposium on Usable Privacy and Security*, 2009, pp. 1–12.
- [22] P. G. Kelley, L. Cesca, J. Bresee, and L. F. Cranor, "Standardizing privacy notices: an online study of the nutrition label approach," in *Proceedings of the SIGCHI Conference on Human factors in Computing Systems*, 2010, pp. 1573–1582.
- [23] S. Frey, "Get more information about your apps in Google play," <https://blog.google/products/google-play/data-safety/>, 2022.
- [24] A. Developer, "What's new in privacy on the app store," <https://developer.apple.com/news/?id=av1nevon>, 2023.
- [25] G. L. Scoccia, M. Autili, G. Stilo, and P. Inverardi, "An empirical study of privacy labels on the Apple iOS mobile app store," in *Proceedings of the 9th IEEE/ACM International Conference on Mobile Software Engineering and Systems*, 2022, pp. 114–124.
- [26] T. Li, K. Reiman, Y. Agarwal, L. F. Cranor, and J. I. Hong, "Understanding challenges for developers to create accurate privacy nutrition labels," in *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, 2022, pp. 1–24.
- [27] Y. Li, D. Chen, T. Li, Y. Agarwal, L. F. Cranor, and J. I. Hong, "Understanding iOS privacy nutrition labels: An exploratory large-scale analysis of app store data," in *CHI Conference on Human Factors in Computing Systems Extended Abstracts*, 2022, pp. 1–7.
- [28] R. Khandelwal, A. Nayak, P. Chung, and K. Fawaz, "Unpacking privacy labels: A measurement and developer perspective on Google's data safety section," *arXiv preprint arXiv:2306.08111*, 2023.
- [29] I. Psychoula, D. Singh, L. Chen, F. Chen, A. Holzinger, and H. Ning, "Users' privacy concerns in IoT based applications," in *2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDC/IOP/SCI)*. IEEE, 2018, pp. 1887–1894.
- [30] P. Emami-Naeini, S. Bhagavatula, H. Habib, M. Degeling, L. Bauer, L. F. Cranor, and N. Sadeh, "Privacy expectations and preferences in an IoT world," in *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, 2017, pp. 399–412.
- [31] S. Zheng, N. Aphorpe, M. Chetty, and N. Feamster, "User perceptions of smart home IoT privacy," *Proceedings of the ACM on Human-Computer Interaction*, vol. 2, pp. 1–20, 2018.
- [32] E. Zeng, S. Mare, and F. Roesner, "End user security and privacy concerns with smart homes," in *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, 2017, pp. 65–80.
- [33] Y. Shen and P.-A. Vervier, "IoT security and privacy labels," in *Privacy Technologies and Policy: 7th Annual Privacy Forum, APF 2019, Rome, Italy, June 13–14, 2019, Proceedings 7*. Springer, 2019, pp. 136–147.
- [34] A. Railean and D. Reinhardt, "Let there be lite: design and evaluation of a label for IoT transparency enhancement," in *Proceedings of the 20th International Conference on Human-Computer Interaction with Mobile Devices and Services Adjunct*, 2018, pp. 103–110.
- [35] —, "Onlite: on-line label for IoT transparency enhancement," in *Secure IT Systems: 25th Nordic Conference, NordSec 2020, Virtual Event, November 23–24, 2020, Proceedings 25*. Springer, 2021, pp. 229–245.
- [36] P. Caven, Z. Zhang, J. Abbott, X. Ma, and L. Camp, "Comparing the use and usefulness of four IoT security labels," in *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, 2024, pp. 1–31.
- [37] A greener world, "Non-GMO label comparison chart," <https://agreenerworld.org/certifications/certified-nongmo-agw/>, 2019.
- [38] T. C. Institute, "Nestlé sued over "no GMO" label," <https://www.cornucopia.org/2018/08/nestle-sued-over-no-gmo-label/>, 2018.
- [39] United States Government Accountability Office, "Covert testing shows the Energy Star program certification process is vulnerable to fraud and abuse," <https://www.ul.com/news/ul-solutions-named-lead-administrator-first-ever-us-federal-cybersecurity-labeling-program>, March 2010.
- [40] Y.-S. Chiang, "Interpreting IoT labels from around the globe," <https://innovation.consumerreports.org/interpreting-iot-labels-from-around-the-globe>, 2023.
- [41] M. Department for Digital, Culture and Sport, "Code of practice for consumer IoT security," <https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security>, 2018.
- [42] European Standards Organisation, "CYBER; cyber security for consumer Internet of Things," https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf, 2019.
- [43] —, "CYBER; cyber security for consumer Internet of Things: Baseline requirements," https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf, 2020.
- [44] H. Hennessey and M. Sullivan-Trainor, "Consumer IoT device cybersecurity standards, policies, and certification schemes," <https://csa-iot.org/wp-content/uploads/2023/02/Consumer-IoT-Device-Cybersecurity-Standards-Policies-and-Certification-Schemes.pdf>, 2023.
- [45] P. J. Caven, S. Gopavaram, J. Dev, and L. J. Camp, "SoK: Anatomy of effective cybersecurity label development," *Available at SSRN 4591786*, 2023.
- [46] Cyber Security Agency of Singapore (CSA), "Cybersecurity labelling scheme," <https://form.gov.sg/5f7b2234956eff0011c006c5>, 2020.
- [47] F. Richter, "How smart are American homes?" <https://www.statista.com/chart/31247/smart-home-adoption-in-the-united-states>, 2023.
- [48] A. Vigderman, "Smart home consumer trends and shopping insights: 2021," <https://www.security.org/smart-home/consumer-shopping-insights/>, 2021.
- [49] Department of Home Affairs, "Stay smart: Helping consumers choose cyber secure smart devices," <https://behaviouraleconomics.pmc.gov.au/projects/stay-smart-helping-consumers-choose-cyber-secure-smart-devices>, 2021.
- [50] F. Faul, E. Erdfelder, A.-G. Lang, and A. Buchner, "G* power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences," *Behavior research methods*, vol. 39, no. 2, pp. 175–191, 2007.
- [51] I. Phau, M. Sequeira, and S. Dix, "Consumers' willingness to knowingly purchase counterfeit products," *Direct Marketing: An International Journal*, vol. 3, no. 4, pp. 262–281, 2009.
- [52] R. L. Oliver and W. O. Bearden, "Crossover Effects in the Theory of Reasoned Action: A Moderating Influence Attempt," *Journal of Consumer Research*, vol. 12, no. 3, pp. 324–340, 1985. [Online]. Available: <https://doi.org/10.1086/208519>

- [53] V. A. Zeithaml, L. L. Berry, and A. Parasuraman, "The behavioral consequences of service quality," *Journal of marketing*, vol. 60, no. 2, pp. 31–46, 1996.
- [54] E. Delgado-Ballester and J. L. Munuera-Alemán, "Brand trust in the context of consumer loyalty," *European Journal of marketing*, vol. 35, no. 11/12, pp. 1238–1258, 2001.
- [55] C. Pinson and D. J. Brosdahl, "The church of Mac: Exploratory examination on the loyalty of Apple customers," *Journal of Management and Marketing Research*, vol. 14, p. 1, 2014.
- [56] P. Caven, A. Gurjar, Z. Zhang, X. Ma, and L. Camp, "Usability, efficacy, and acceptability of the us cyber trust mark," in *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, 2025, pp. 1–35.
- [57] "Finnish Transport and Communications Agency (Traficom)," 2023. [Online]. Available: <https://tietoturvamerkki.fi/en/products>
- [58] Federal Office for Information Security, "Questions and answers for costumers for the IT Security Label," https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/IT-SiK-fuer-Verbraucher/FAQ-IT-SiK-fuer-Verbraucher/faq_it-sik-verbraucher_node.html.

APPENDIX

Understanding smart device label behaviors and preferences

What is the purpose of this study? You are being asked to participate in a voluntary research study. This research aims to understand people's attitudes for smart home devices labels. Participating in this study will involve a survey, and your participation will last approximately 5 minutes. There are no foreseeable risks to you beyond those normally encountered in your daily life while participating in this survey. Your response to this survey will provide us with insights that can contribute to the future data collection policy. If you agree to participate, you will be asked to check "I consent" at the bottom of this page indicating that you have read the following form and have been shown the goals of this study. What will happen during this study? This study includes a single survey where you will be presented with a scenario and be asked questions about your opinions. **Will my study-related information be kept confidential?** We will use all reasonable efforts to keep your personal information confidential, but we cannot guarantee absolute confidentiality. When this research is discussed or published, no one will know that you were in the study. Faculty, students, and staff who may see your information will maintain confidentiality to the extent of laws and university policies. Personal identifiers will not be published or presented. We will remove all identifiers or paraphrase your responses if we were to quote your answer in any publication.

Will I be reimbursed for any expenses or paid for my participation in this research? You will receive \$1.0 after completing the study via Prolific and the researchers confirmed the attention check question and completion code.

Can I withdraw or be removed from the study? If you decide to participate, you are free to withdraw your consent and discontinue participation at any time. Your participation in this research is voluntary.

Will data collected from me be used for any other research? Your de-identified information could be used for future research without additional informed consent.

Who should I contact if I have questions? If you have questions about this project, you may contact [Redacted name

for anonymity] at [Redacted email for anonymity]. Please print this consent form if you would like to retain a copy for your records.

I have read and understood the above consent form. I certify that I am 18 years old or older. By clicking the "I consent" button to enter the survey, I indicate my willingness to voluntarily take part in this study. If you click "No, I do not consent", you will be directed to the end of the survey, your data will not be saved, and you will not receive compensation for participating.

- Yes, I am 18 year old or older and consent to participate in the study.
- No, I am younger than 18 years old or I do not consent.

There are seven conditions in total. Here we provided an example of level 1 from the layered label program.

About IoT labels

To increase the security and privacy transparency of smart home devices, the government launched a **voluntary** labeling system. Manufacturers are encouraged to apply when they have met the security requirements, such as ensuring the software integrity and data safety.

IoT labels awarding policy The manufacturers will be awarded the label of different levels once the product has met the corresponding requirements. There are two levels:

Level 1: The products will be given a level 1 label once the manufacturers have self-declared compliance with all requirements and application materials.

Level 2: The product will be awarded with a level 2 label when the product's compliance with all requirements has passed third-party inspection.

These are the labels of different levels.



This is the full list of security requirements: (1) No universal default passwords, (2) Implement a means to manage reports of vulnerabilities, (3) Keep software updated, (4) Securely store credentials and security-sensitive data, (5) Communicate securely, (6) Minimise exposed attack surfaces, (7) Ensure software integrity, (8) Ensure that personal data is protected, (9) Make systems resilient to outages, (10) Examine system telemetry data, (11) Make it easy for consumers to delete personal data, (12) Make installation and maintenance of devices easy, (13) Validate input data.

When looking at the package, you realize that this product **does** have a level 1 IoT label on the bottom left of the front of the package (Figure 7).

How **concerned** are you about the **security** protection of the product?

- Concerned
- Somewhat concerned
- Neither concerned nor not concerned
- Somewhat not concerned



Fig. 7. Image of a smart speaker product with a Level 1 label.

- Not concerned

How **concerned** are you about the **privacy** aspects of the product?

- Concerned
- Somewhat concerned
- Neither concerned nor not concerned
- Somewhat not concerned
- Not concerned

How easy or difficult is it for you to **understand the label**?

- Easy
- Somewhat easy
- Neither easy or difficult
- Somewhat difficult
- Difficult

How **informative** do you think this label is to you?

- Informative
- Somewhat informative
- Neither informative or not informative
- Somewhat not informative
- Not informative

Select the IoT awarding mechanism that you find the most trustworthy:

- The label should be **mandatory with no expectation**: All device should get certified
- The label should be **mandatory with few expectations**: In principle, devices should all get certified; few devices that do not collect personal identifying information and bioinformatics can apply for exemptions
- The label should be **voluntary with few expectations**: In principle, devices do not need to get certified; devices that do collect personal identifying information and bioinformatics are required to be certified
- The label should be **voluntary with no expectation**: All devices are not required to get certified

Due to the confusing typo in the answer choices for the question above, we have omitted this question from our results.

Which of these devices do you use in your home? Select all that apply.

- ☐ Smart speaker (e.g., Google Home, Amazon Alex)

- ☐ Smart cameras (e.g., Smart doorbell with camera, smart baby monitor, smart pet monitor)
- ☐ Smart security (e.g., smart lock, smart garage door closer, smart security system)
- ☐ Smart TV (e.g., Apple TV)
- ☐ Smart media player (e.g., Roku, Chromecast)
- ☐ Smart home management (e.g., smart thermostat, smart light bulb, smart outlet)
- ☐ Standalone smart appliance (e.g., smart refrigerator, smart coffee maker)
- ☐ Smart wearable device (e.g., smart watch, smart fitness tracker)
- ☐ Other (please specify)
- ☐ Does not apply; I do not have any smart device

Where do you usually purchase smart devices? Select the one you use the most often.

- Physical stores (e.g., Walmart, Target, Bestbuy)
- Online shops (e.g. Amazon, Target, Google shops, eBay, manufacturer's website)
- Bundles[Sic: Bundles] or special offers from utility, alarm, cable companies (e.g. AT&T, Ameren)
- Other (please specify)
- Does not apply; I do not have any smart device

Are you in the market for buying smart devices? Select all that apply.

- ☐ Smart speaker (e.g., Google Home, Amazon Alex)
- ☐ Smart cameras (e.g., Smart doorbell with camera, smart baby monitor, smart pet monitor)
- ☐ Smart security (e.g., smart lock, smart garage door closer, smart security system)
- ☐ Smart TV (e.g., Apple TV)
- ☐ Smart media player (e.g., Roku, Chromecast)
- ☐ Smart home management (e.g., smart thermostat, smart light bulb, smart outlet)
- ☐ Standalone smart appliance (e.g., smart refrigerator, smart coffee maker)
- ☐ Smart wearable device (e.g., smart watch, smart fitness tracker)
- ☐ Other (please specify)
- ☐ Does not apply; I do not have any smart device

When you were buying smart devices, what information did you search for when making buying decisions? And how hard is it to search for the information? See Figure 8.

If you have searched for any of the aforementioned information. How did you search for them? Select all that apply.

- ☐ Product packaging or in a store
- ☐ Manufacturer's website
- ☐ A retailer product page (e.g. Amazon, Best Buy, Target)
- ☐ Product reviews or news articles (e.g., Consumer Reports, CNET, Wirecutter)
- ☐ Word of mouth (e.g. friends, colleagues, neighbors)
- ☐ Does not apply; I have not searched for any of this information
- ☐ Other (please specify)

What is your age?

	Difficult	Somewhat difficult	Neither easy nor difficult	Somewhat easy	Easy	Does not apply; I did not search for this information
Password and account access policy: Installation and maintenance of the device should involve minimal decisions by the user and should follow security best practice on usability.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Vulnerability report system: The manufacturers have a public channel for people to report product vulnerabilities.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Software update availability and schedule: The product will be eligible for future software updates and how long the product will be supported	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Securely store credentials and security-sensitive data: The credential and security-sensitive data collected by the product will be stored securely	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Communicate securely: The devices communicates with other devices and the device securely	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Minimise exposed attack surfaces: The network interfaces of the device shall minimize the unauthenticated disclosure of security-relevant information.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ensure software integrity: The device should verify its software using secure mechanisms.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ensure that personal data is protected: The confidentiality of personal data transiting between a device and a service should be protected with best practice cryptography.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Make systems resilient to outages: The devices should remain operating and locally functional in the case of a loss of network access and should recover cleanly in the case of restoration of a loss of power.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Examine system telemetry data: If telemetry data is collected from the devices and services, such as usage and measurement data, it should be examined for security anomalies.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Make it easy for consumers to delete personal data: The consumer should be provided with functionality on the device such that personal data can be removed from associated services in a simple manner.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Make installation and maintenance of devices easy: Installation and maintenance of the devices should involve minimal decisions by the user and should follow security best practices on usability.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Validate input data: The device software shall validate data input via user interfaces or transferred via Application Programming Interfaces (APIs) or between networks in services and devices.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Fig. 8. Participants reported they have search for ETSI EN 303 645 required information. If yes, how difficult it is find each piece of information.

- ☐ 18-24
 - ☐ 25-34
 - ☐ 35-44
 - ☐ 45-54
 - ☐ 55-64
 - ☐ 65 and above
 - ☐ Prefer not to answer
- What is the highest level of formal education that you have completed?
- ☐ Less than a high school diploma
 - ☐ High school degree or equivalent (e.g., GED)
 - ☐ Associate degree (e.g., AA, AS)
 - ☐ Bachelor's degree (e.g., BA, BS)
 - ☐ Master's degree (e.g. MA, MS, MEd)
 - ☐ Professional degree (e.g. MD, DDS, DVM)
 - ☐ Doctorate (e.g. PhD, EdD)
 - ☐ Prefer not to answer
- Please indicate the answer that includes your entire household income in (previous year) before taxes.
- ☐ Less than \$10,000
 - ☐ \$10,000 - \$19,999
 - ☐ \$20,000 - \$29,999
 - ☐ \$30,000 - \$39,999
 - ☐ \$40,000 - \$49,999
 - ☐ \$50,000 - \$59,999
 - ☐ \$60,000 - \$69,999
 - ☐ \$70,000 - \$79,999
 - ☐ \$80,000 - \$89,999
 - ☐ \$90,000 - \$99,999
 - ☐ \$100,000 - \$149,999
 - ☐ \$150,000 or more
 - ☐ Prefer not to answer
- What is the gender you identify with?
- ☐ Male

- Female
- Non-binary
- Prefer not to say