

Is a Trustmark and QR Code Enough? The Effect of IoT Security and Privacy Label Information Complexity on Consumer Comprehension and Behavior

Claire C. Chen
Carnegie Mellon University
Pittsburgh, PA, USA
clairechen@cmu.edu

Xinran Li
Carnegie Mellon University
Pittsburgh, PA, USA
xinranl2@andrew.cmu.edu

Dillon Shu
Carnegie Mellon University
Pittsburgh, PA, USA
dillons@andrew.cmu.edu

Yuvraj Agarwal
Carnegie Mellon University
Pittsburgh, PA, USA
yuvraj@cs.cmu.edu

Hamsini Ravishankar
Carnegie Mellon University
Pittsburgh, PA, USA
hravisha@andrew.cmu.edu

Lorrie Faith Cranor
Carnegie Mellon University
Pittsburgh, PA, USA
lorrie@cmu.edu

ABSTRACT

The U.S. Government is developing a package label to help consumers access reliable security and privacy information about Internet of Things (IoT) devices when making purchase decisions. The label will include the U.S. Cyber Trust Mark, a QR code to scan for more details, and potentially additional information. To examine how label information complexity and educational interventions affect comprehension of security and privacy attributes and label QR code use, we conducted an online survey with 518 IoT purchasers. We examined participants' comprehension and preferences for three labels of varying complexities, with and without an educational intervention. Participants favored and correctly utilized the two higher-complexity labels, showing a special interest in the privacy-relevant content. Furthermore, while the educational intervention improved understanding of the QR code's purpose, it had a modest effect on QR scanning behavior. We highlight clear design and policy directions for creating and deploying IoT security and privacy labels.

CCS CONCEPTS

• **Security and privacy** → **Usability in security and privacy**; • **Social and professional topics** → *Governmental regulations*.

KEYWORDS

Privacy, Security, Smart Environments / Connected Home, Ambient Devices / Internet of Things

ACM Reference Format:

Claire C. Chen, Dillon Shu, Hamsini Ravishankar, Xinran Li, Yuvraj Agarwal, and Lorrie Faith Cranor. 2024. 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 CHI Conference on Human Factors in Computing Systems (CHI '24)*, May 11–16, 2024,



This work is licensed under a Creative Commons Attribution International 4.0 License.

CHI '24, May 11–16, 2024, Honolulu, HI, USA
© 2024 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-0330-0/24/05
<https://doi.org/10.1145/3613904.3642011>

Honolulu, HI, USA. ACM, New York, NY, USA, 32 pages. <https://doi.org/10.1145/3613904.3642011>

1 INTRODUCTION

Security and privacy vulnerabilities of Internet of Things (IoT) products have long been exploited, resulting in leakage of personal information and eavesdropping of communication between devices [2, 28], attackers taking over control of smart devices remotely leading to physical risks [11], unauthorized sensing and data collection, and use of personal information [4, 6, 37, 42]. Users have expressed concerns over security risks and privacy-invasive data practices of IoT devices [19, 29] but find it difficult to act on these concerns, thereby putting themselves at risk [12]. Proposals for security and privacy labels affixed to the IoT packaging show promise as an effective means of educating users about IoT security and privacy practices and promoting more informed device purchase decisions [19].

The United States government has been working towards the establishment of an IoT security and privacy labeling program for several years. In 2021, Executive Order 14028 tasked the National Institute of Standards and Technology (NIST) with developing a cybersecurity baseline for IoT products [25]. NIST subsequently issued a white paper that included basic criteria for labeling [47]. In October 2022, the White House convened representatives from the U.S. government, industry, and academia to discuss ideas for a national cybersecurity labeling program for IoT devices [26]. In July 2023, the White House announced a voluntary IoT cybersecurity labeling program and unveiled a “U.S. Cyber Trust Mark” that would certify the fulfillment of basic cybersecurity criteria [27]. A month later, the Federal Communications Commission (FCC) issued a Notice of Proposed Rulemaking (NPRM) soliciting public comments on a framework for a layered binary label including the U.S. Cyber Trust Mark and a QR code that can be scanned for information about specific IoT devices [8].

Previous research has focused on the design of IoT labels based on input from experts and iterative consumer testing [15, 19]. Emami-Naeini et al. proposed and evaluated a two-layer label design comprising a primary layer with the most salient security and privacy attributes for consumers and a QR code at the bottom leading to a

more comprehensive secondary layer designed for experts [14, 16–18]. However, IoT manufacturers have advocated for minimal labels that include only a Cyber Trust Mark and QR code, citing limited space on product packaging. Prior work has neither compared consumer preferences for minimal versus more expansive labels nor evaluated the comparative effectiveness of these approaches.

Our research aims to shed light on consumer preferences for, and the effectiveness of, three designs of varying complexity for IoT security and privacy labels on product packaging. Specifically, we investigate the following research questions:

- RQ1: What is the impact of complexity level on consumers' understanding of the information on the labels?
- RQ2: What is the impact of complexity level on consumers' interactions with labels (a) during the study and (b) their self-reported expected future interactions with labels?
- RQ3: What is the impact of complexity level on consumers' preferences for the labels?
- RQ4: Which label attributes do consumers report would most influence their decisions to purchase IoT devices?
- RQ5: What is the impact of (a) a brief educational intervention, (b) age, (c) gender, and (d) technical background on consumer understanding, interactions, and preferences for the three labels studied?

We conducted an online survey of 518 purchasers of IoT devices to examine their preferences about the complexity of the labels on device packaging, their ability to use these on-package labels, as well as labels accessed through a QR code. We created a high-complexity label and an ultra-high-complexity label based on Emami-Naeini et al.'s label designs and the U.S. Cyber Trust Mark. We created a low-complexity label that included only a QR code and the U.S. Cyber Trust Mark. We also created a medium-complexity label that added a few of the most important elements from the high-complexity label to the minimal low-complexity design.

We assigned participants randomly to the low-, medium-, or high-complexity level and showed them labels for three functionally identical IoT devices (smart thermostats) with differing security and privacy properties under fictitious brand names. In addition, we randomly assigned half of the participants in each complexity group to view a brief educational intervention introducing the Trust Mark and QR code prior to beginning the survey. We asked participants questions to assess their comprehension of the labels and their ability to use them to compare products. As shown in Figure 1, participants who chose to scan the QR code on a label in the survey were redirected to a website displaying a higher complexity label. Once on the website, participants could interact with the label to obtain further information until they reached the ultra-high-complexity label. At the end of the survey, we showed participants labels from all four complexity levels and asked them about their most preferred label option.

We found that most participants did not scan the QR code, even when asked to answer questions based on seeing only the low-complexity label containing nothing but the QR code and the Trust Mark. Participants generally favored labels with more information, and preferred to have that information readily available on the package itself rather than only accessible by scanning a QR code. Less than 2% of participants preferred the low-complexity label when

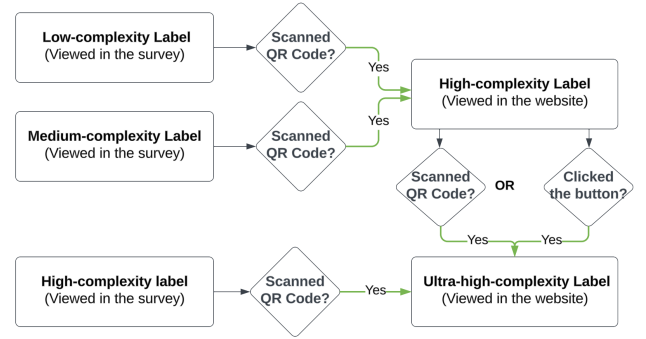


Figure 1: Possible participant interactions with the labels.

given a choice between labels. Our results also indicate that those who received a brief educational intervention at the beginning of the survey had a better understanding of the Cyber Trust Mark and the QR code. Despite this, the effect of education on motivating them to scan the QR code was limited. Participants were most interested in seeing labels that included information about the devices' sensors, data collection and purposes, data sharing practices, and information about security updates.

We recommend that as policymakers define requirements for products to receive the U.S. Cyber Trust Mark and consider designs for accompanying IoT labels, they focus on label designs similar to our medium- and high-complexity labels. These designs should provide both security and privacy information important for consumer decision-making on product packaging and use QR codes to provide more detailed information. As designs are refined, they should be informed with further consumer testing. Finally, we recommend sustained educational campaigns and in-store signage to inform consumers about the U.S. Trust Mark and how to use the accompanying label to make informed purchase decisions.

2 BACKGROUND AND RELATED WORK

We first discuss security threats to IoT devices. We then introduce the concept of labels and discuss prior work on the design and evaluation of labels in privacy and security contexts, particularly IoT devices. We end with a brief review of recent government and industry efforts to standardize IoT security and privacy labels.

IoT security and privacy threats. IoT device owners are susceptible to security breaches that may result in unintended exposure of personal or private information, including daily activities monitored by device sensors [1, 58, 59]. Numerous cybersecurity attacks targeting IoT devices have been recorded, such as the Mirai botnet incident in 2016, when a worm-like family of malware named Mirai launched massive distributed denial-of-service (DDoS) attacks, resulting in 600k infections at its peak, and brought down many popular websites [1, 30]. Mirai has since inspired more advanced IoT botnets [24]. Despite the security and privacy risks associated with IoT devices, details about device security and privacy are generally not available to consumers. As a result, consumers often purchase IoT devices without knowing about the potential privacy and security risks associated with them or which devices include features that may help mitigate risks [29, 44]. Recent studies have

shown that consumers want information about security and privacy when making smart device purchases but lack a reliable means to access this information [19, 22, 60].

IoT labels. Labels communicate standardized information about consumer goods in a concise and organized manner. For example, nutrition facts and drug facts labels have helped consumers make informed purchasing decisions about food and pharmaceuticals. Past research has demonstrated that privacy labels on websites are more effective at aiding comprehension and enabling easy access to information than traditional text-based privacy policies [31, 32, 35]. Kelley et al. developed an Android app privacy label and found that study participants who were presented with labels in the app store often chose more privacy-protective apps than those not shown the labels [33]. More recently, privacy labels have been introduced in both iOS and Android app stores. However, studies have found their terminology and layouts can confuse both consumers and app developers [9, 39, 40, 61], suggesting extensive user testing is needed in the development of new labels.

Railean and Reinhardt developed and evaluated a “Privacy facts” label for the European context that included information about an IoT device’s sensors, data collection, data recipients, data processing purposes, retention periods, and data flows. Their label also included a QR code leading to actual data samples [50, 51].

Emami-Naeini et al. interviewed U.S. consumers about their needs for both security and privacy information when purchasing IoT devices [19]. They also interviewed IoT security and privacy experts about the information most important for making an informed purchase decision [15]. Using what they learned from experts and consumers, they developed a two-layer IoT label for the U.S. context and showed that it is both usable and informative for consumers [16]. In their CMU IoT Security and Privacy Label (CISPL) design, the primary layer contains the information that is most salient to consumers and a QR code leading to a more detailed secondary layer that adds additional information of interest to experts. In subsequent work, the authors demonstrated consumers accurately differentiated between more and less risky attributes included on the labels and that label information impacted their willingness to purchase IoT devices [17]. In their most recent work, Emami-Naeini et al. demonstrated that consumers would be willing to pay a significant premium for more secure and private IoT devices, as compared to devices with bad practices or those without any disclosures, if security and privacy information was disclosed and made readily available [18].

Label regulation and policy. Governments worldwide have taken steps to promote, enforce, and standardize the use of IoT privacy labels [16, 19]. The CISPL specification provides a list of device security and privacy attributes and associated global standards [57]. Finland and Singapore have recently developed IoT label standards [46, 55]. Singapore uses a tiered rating system (1 to 4 stars) based on requirements set forth by ETSI 303 645, which is the European security standard for IoT devices [10]. The 1-star rating requires meeting the baseline ETSI standard while the 3- or 4-star ratings are given for independent verification and binary analysis by test labs and penetration testing by separate third parties respectively [45]. Germany and Finland have a reciprocal arrangement for their own IoT schemes which recognize devices that meet the Singapore standard, and vice versa [46]. Recently, the European

Union passed the Cyber Resilience Act [56] that addresses cybersecurity of connected devices. The expectation is that additional security requirements will be added to existing requirements that manufacturers have to meet to get the European “CE Mark,” which signifies that a product meets various safety, health, and environmental requirements. It is not clear whether the E.U. will require adding a QR code or include any other information besides the CE Mark.

In response to the U.S. White House Executive Order 14028 in 2021, the National Institute of Standards and Technology (NIST) developed criteria for an IoT products labeling program [25, 43, 47]. Subsequently, the U.S. Federal Communications Commission (FCC) unveiled the Cybersecurity Labeling Program for smart devices, including the U.S. Cyber Trust Mark. The Mark is intended to help Americans make informed choices about smart devices by indicating which devices meet a set of baseline criteria and providing additional security and privacy details via a QR code on product packaging. In August 2023, the FCC solicited input on the details of the label that will accompany the Mark on product packaging as well as the more detailed label accessible through the QR code [7, 27].

The Consumer Technology Association (CTA) has convened working groups in an effort to reach a consensus on details of the U.S. Cyber Trust Mark program and has announced plans to submit comments to the FCC [3]. The authors have observed that some IoT device manufacturers and retailers who are participating in these working groups have expressed concerns about space constraints when placing labels on physical product packaging and are advocating for compact package labels that include only the Cyber Trust Mark and a QR code. This research contributes to the discussion by providing empirical data on consumer preferences for labels of varying complexity as well as the impact of label complexity on consumer comprehension and behavior.

3 METHODS

In this section, we detail our pilot studies, participant recruitment, label design, survey protocol, and data analysis process.

Ethical considerations. Our study protocols were reviewed and approved by the Carnegie Mellon University Institutional Review Board (IRB). All study participants provided their consent using online forms approved by our IRB. As the study was conducted using the Prolific platform, we collected participants’ Prolific IDs to facilitate payment. We collected no other personally identifiable information from participants, and we do not know the real-world identities associated with Prolific IDs.

3.1 Pilot Studies

We conducted pilot studies in the Spring and early Summer of 2023 that helped us iteratively refine our study protocol and label designs. These studies employed protocols fairly similar to the one used in our final study, described below. In addition to differences in label content and design, question format, and purchasing scenarios, our preliminary studies did not include functional QR codes or the U.S. Cyber Trust Mark (announced after these pilot studies).



Figure 2: Low-complexity IoT label for Sustios, a fictional smart thermostat.

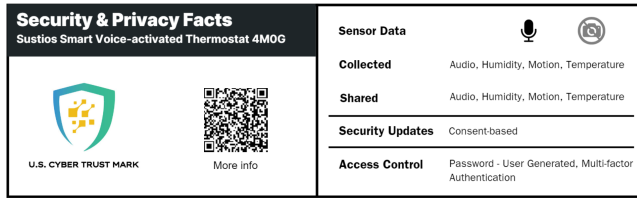


Figure 3: Medium-complexity IoT label for Sustios, a fictional smart thermostat.

3.2 Participant Recruitment

We conducted an online study of U.S.-based IoT device purchasers recruited on Prolific. To achieve a more representative sample through stratified sampling, we utilized Prolific’s gender-balanced distribution feature and recruited a similar number of participants from three different age groups (18-35, 36-53, 54+), roughly proportionate to the U.S. age and gender distribution.¹ Using Prolific’s built-in prescreening tools, the posts were shown only to self-reported IoT device owners of a predetermined list of qualifying devices (see Appendix C). All participants were then redirected to the same prescreen survey. Participants who claimed to have purchased at least one IoT device in the past three years were then given a link to the main survey. Participants received \$0.50 (median of \$9/hour) as compensation for completing the prescreening survey and an additional \$5 (median of \$25/hour) for the main survey.

3.3 Label Design

We tested three IoT security and privacy label designs, which we refer to as low-, medium-, and high-complexity labels (see Figures 2, 3, and 4). Each label included the U.S. Cyber Trust Mark and a QR code that users could scan to retrieve a more detailed label. Users who scanned the low-complexity and medium-complexity labels were shown the high-complexity label, and users who scanned the high-complexity label were shown an even more detailed label, which we refer to as the “ultra-high-complexity label” (see Figure 5). At the end of the study, participants were shown labels of all four complexity levels and asked which they would prefer to see on product packages.

Our label designs were based on the primary and secondary labels proposed by Emami-Naeini et al. [14, 15]. We used the primary layer of CISPL as our high-complexity label, which linked

¹<https://www.census.gov/data/tables/2022/demo/age-and-sex/2022-age-sex-composition.html>

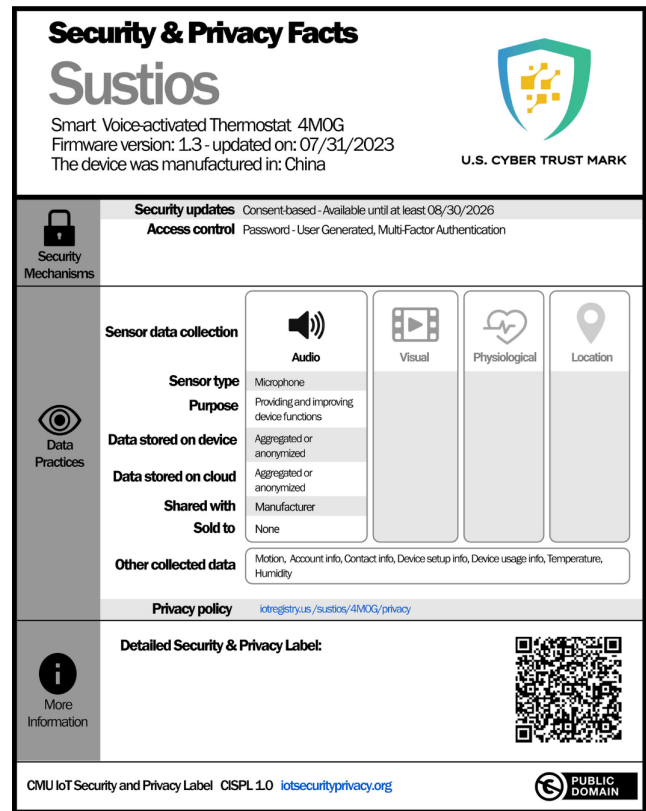


Figure 4: High-complexity IoT label for Sustios, based on the CISPL primary layer design [15, 57].

to our ultra-high complexity label based on the CISPL secondary layer when the QR code was scanned. After receiving feedback from pilot studies that the QR code on the high-complexity label was difficult to scan, we made some small alterations to the label layout to increase the size of the QR code and the quiet zone around it. Additionally, we added a button next to the QR code on the high-complexity labels displayed after scanning so that participants could click to conveniently retrieve the ultra-high complexity label (see Appendix E).

To develop the medium-complexity label, we focused on four attributes that Emami-Naeini et al. found to be strongly associated with increasing consumers’ willingness to purchase, including two security attributes (*security updates* and *access control*) and two privacy attributes (*data collected* and *data shared*) [17]. We also included symbols indicating the presence or absence of cameras or microphones in response to proposed U.S. legislation requiring internet-connected devices to disclose camera or audio recording capabilities [53]. Based on feedback gathered from pilot surveys, we iteratively enhanced the medium-complexity label, which serves as a middle ground between the comprehensive high-complexity label and the minimal low-complexity label.

We designed the low-complexity label to show only the U.S. Cyber Trust Mark and a QR code, which, if scanned, would lead to more detailed information. It was formatted exactly the same as

Security & Privacy Details
Sustios
 Smart Voice-activated Thermostat 4MOG
 Firmware version: 1.3 - updated on: 07/31/2023
 The device was manufactured in: China

Security Mechanisms

Security updates	Consent-based - Available until at least 08/30/2026
Access control	Password - User Generated, Multi-Factor Authentication
Security oversight	www.thermostat.sustios.com/security_audits
Ports and protocols	www.thermostat.sustios.com/ports
Hardware safety	www.thermostat.sustios.com/hw_safety
Software safety	www.thermostat.sustios.com/sw_safety
Personal safety	www.thermostat.sustios.com/personal_safety
Vulnerability disclosure and management	www.thermostat.sustios.com/vul_report
Software and hardware composition list	www.thermostat.sustios.com/BOM
Encryption and key management	www.thermostat.sustios.com/encryption

Data Practices

Sensor data collection	Audio	Motion
Sensor type	Microphone	Motion sensor
Collection frequency	When an event happens	When an event happens
Purpose	Providing and improving device functions	Providing and improving device functions
Data stored on the device	Aggregated or anonymized	Aggregated or anonymized
Local data retention time	No retention	No retention
Data stored in the cloud	Aggregated or anonymized	Aggregated or anonymized
Cloud data retention time	No retention	No retention
Data shared with	Manufacturer	Manufacturer
Data sharing frequency	Continuous	Continuous
Data sold to	None	None
Other collected data	Account info, Contact info, Device setup info, Device usage info, Temperature, Humidity	
Data linkage	Data will not be linked with other data sources	
What will be inferred from user's data	No data inference	
Special data handling practices for children	Yes	
In compliance with	GDPR	
Privacy policy	iortegistry.us/sustios/4MOG/privacy	

More Information

Call Sustios with your questions at	1.000-000-0000
Email Sustios with your questions at	info@sustios.com
Functionality when offline	Limited functionality
Functionality with no data processing	Limited functionality
Physical actuations and triggers	Device blinks when motion is detected
Compatible platforms	Mobile App, Amazon Alexa, Siri, Google Assistant

CMU IoT Security and Privacy Label CISPL 1.0 iotsecurityprivacy.org

Figure 5: Ultra-high-complexity label for Sustios, based on the CISPL secondary layer [15, 57].

the left side of the medium-complexity label. This design mirrors what was shown during the U.S. Cyber Trust Mark launch in 2023 [7, 27], as one that would likely be used on product packaging given space constraints discussed by IoT device manufacturers and trade associations.

3.4 Survey Design

We conducted a between-subjects survey in which one-third of the participants were randomly assigned to each label complexity level. For each of these three groups, we provided a brief educational intervention to half of the participants. The intervention (shown in Appendix B) included an image of the U.S. Cyber Trust Mark, a brief explanation of its significance, and a note that consumers can “scan the accompanying QR code to get more information about the product’s security and privacy attributes.” At the bottom of the intervention page were two questions testing participants’ comprehension of the purpose of the U.S. Cyber Trust Mark and QR code. We implemented the survey such that only respondents

Security & Privacy Facts
 Sustios Smart Voice-activated Thermostat 4MOG

Sensor Data

Collected	Audio, Humidity, Motion, Temperature
Shared	Audio, Humidity, Motion, Temperature
Security Updates	Consent-based
Access Control	Password - User Generated, Multi-factor Authentication

(a) Medium-complexity label for Sustios

Security & Privacy Facts
 All4Home Smart Voice-activated Thermostat 5H23B

Sensor Data

Collected	Audio, Humidity, Motion, Temperature
Shared	Audio, Humidity, Motion, Temperature
Security Updates	Manual
Access Control	Password - User Generated

(b) Medium-complexity label for All4home

Security & Privacy Facts
 EcoHouse Smart Voice-activated Thermostat E40

Sensor Data

Collected	Audio, Humidity, Motion, Temperature, Video
Shared	Audio, Humidity, Motion, Temperature, Video
Security Updates	None
Access Control	Password - Factory default - User changeable

(c) Medium-complexity label layer for EcoHouse


Figure 6: Medium-complexity labels for the three smart thermostats. Sustios has the best privacy and security attributes, followed by All4home. EcoHouse has the worst security and privacy attributes. The low-complexity labels were formatted the same as the left side of the medium-complexity labels.

who answered both questions accurately could proceed to the next section. Participants were permitted to change their answers until they were able to answer both questions correctly.


Participants were presented with labels using their assigned complexity label for three fictional IoT thermostats with identical functionality but varying security and privacy attributes. As shown in Figure 6 for the medium-complexity group and Figure 7 for the high-complexity group, the three IoT thermostats included a device with strong privacy and security features, a device with medium privacy and security, and a device with weak privacy and security. We tried to select strong and weak values that could be clearly distinguishable by non-experts (e.g., more sharing implies weaker privacy than less sharing, and consent-based security updates are stronger than no security updates). To prevent external factors from influencing participants’ decisions, we chose fictitious brand names that were distinct from existing brands.

We generated a unique QR code for each participant with QR-Code.js [52], overlaid on top of the labels through Qualtrics, directing those who scanned to a label hosted on our research group’s web server. This enabled us to track participant scanning through the unique URLs that appeared in our weblogs.


The survey included multiple-choice questions, Likert scale questions, and open-ended questions to quantitatively and qualitatively

Security & Privacy Facts		Sustios		U.S. CYBER TRUST MARK	
Smart Voice-activated Thermostat 4MOG Firmware version: 1.3 - updated on: 07/31/2023 The device was manufactured in: China					
Security Mechanisms	Security updates	Consent-based - Available until at least 08/30/2026			
	Access control	Password - User Generated, Multi-Factor Authentication			
Data Practices	Sensor data collection	<div>Audio</div> <div>Visual</div> <div>Physiological</div> <div>Location</div>			
	Sensor type	Microphone			
	Purpose	Providing and improving device functions			
	Data stored on device	Aggregated or anonymized			
	Data stored on cloud	Aggregated or anonymized			
	Shared with	Manufacturer			
	Sold to	None			
	Other collected data	Motion, Account info, Contact info, Device setup info, Device usage info, Temperature, Humidity			
Privacy policy		iotregistry.us/sustios/4MOG/privacy			
More Information	Detailed Security & Privacy Label:				
					
CMU IoT Security and Privacy Label CISPL 1.0 iotsecurityprivacy.org PUBLIC DOMAIN					

(a) High-complexity label for Sustios

Security & Privacy Facts		EcoHouse		U.S. CYBER TRUST MARK	
Smart Voice-activated Thermostat E40 Firmware version: 1.0 - updated on: 04/12/2021 The device was manufactured in: China					
Security Mechanisms	Security updates	None			
	Access control	Password - Factory default - User changeable			
Data Practices	Sensor data collection	<div>Audio</div> <div>Visual</div> <div>Physiological</div> <div>Location</div>			
	Sensor type	Microphone			
	Purpose	Providing and improving device functions, Tailored advertising and monetization, Tailored individualized experiences.			
	Data stored on cloud	Identified			
	Data stored on device	Identified			
	Shared with	Manufacturer, Government, Service providers			
	Sold to	Third Parties			
	Other collected data	Motion, Account info, Contact info, Device setup info, Device usage info, Temperature, Humidity			
Privacy policy		iotregistry.us/EcoHouse/E40/privacy			
More Information	Detailed Security & Privacy Label:				
					
CMU IoT Security and Privacy Label CISPL 1.0 iotsecurityprivacy.org PUBLIC DOMAIN					

(c) High-complexity label for EcoHouse

Security & Privacy Facts		All4Home		U.S. CYBER TRUST MARK	
Smart Voice-activated Thermostat 5H23B Firmware version: 1.2 - updated on: 05/23/2022 The device was manufactured in: China					
Security Mechanisms	Security updates	Manual - Available until at least 06/01/2024			
	Access control	Password - User Generated			
Data Practices	Sensor data collection	<div>Audio</div> <div>Visual</div> <div>Physiological</div> <div>Location</div>			
	Sensor type	Microphone			
	Purpose	Providing and improving device functions, For tailored individualized experiences.			
	Data stored on device	Pseudonymized			
	Data stored on cloud	Pseudonymized			
	Shared with	Manufacturers, Service Providers			
	Sold to	Third Parties, with option to opt out			
	Other collected data	Motion, Account info, Contact info, Device setup info, Device usage info, Temperature, Humidity			
Privacy policy		iotregistry.us/all4home/5H23B/privacy			
More Information	Detailed Security & Privacy Label:				
					
CMU IoT Security and Privacy Label CISPL 1.0 iotsecurityprivacy.org PUBLIC DOMAIN					

(b) High-complexity label for All4home

Figure 7: High-complexity labels for three smart thermostats. Sustios has the best privacy and security attributes, followed by All4home. EcoHouse has the worst security and privacy attributes.

assess participant comprehension of label information, perception of the usefulness of label information, and ease or difficulty using the labels and QR codes. Near the end of the survey, we presented participants with the low-, medium-, high-, and ultra-high-complexity labels and asked them which one they preferred to see on the product packaging and upon scanning a QR code. Finally, we asked them to rate the importance of various factors when purchasing an IoT device (Q31) and to indicate their agreement with four statements about their security and privacy behavior (Q32). As we wanted to ask only a few questions and have coverage of both security- and privacy-related behaviors, we did not use an established scale [13] but instead included four questions to cover the tendency to read privacy policies, motivation to keep accounts safe (from SA-6) [20], cookie blocking, and use of two-factor authentication. We provide all of our survey questions in Appendix A.

3.5 Data Analysis

We performed a quantitative analysis to look for significant differences between our treatment conditions (label complexity, educational intervention) as well as across demographic groups (age, gender, and technical background). For independent variables with

more than two categories (age, label complexity), we adopted two-stage testing: an overall omnibus, followed by pairwise tests if significant. Independent variables with two categories (education and gender) were tested directly with pairwise tests. For questions (i.e., dependent variables) with multiple-choice responses, we used Fisher's Exact test if more than 20% of the entries in a contingency table have less than or equal to 5 observations [21, 34]. For the remaining multiple-choice questions, which satisfy the Chi-square assumption, we performed Pearson's Chi-squared test [48].

For multi-select questions, we interpreted each of the possible options as a binary multiple-choice question with responses being True or False. We then tested each sub-question for significance using the same procedure as multiple-choice questions with two options.

For Likert-scale questions or numeric-response dependent variables (e.g., number of QR code scans), we measured rank significance across complexity groups and demographic groups using the Kruskal-Wallis omnibus test [36]. If significance has been identified for a specific question across all tested groups, we then performed the Mann-Whitney U test on each pair of groups to determine pairwise significance.

We performed a post hoc Benjamini-Hochberg procedure to all p -values *globally*, in order to control for false discovery rates (FDR) potentially caused by multiple testing [5].

We conducted a qualitative analysis of open-ended responses based on a codebook developed jointly by three authors of this paper. During the formative and pilot studies, two or three authors coded every response while maintaining a high agreement rate. For the main study, two authors independently coded all open-ended questions, agreeing on the codebook and relevant assumptions. After completing the coding process, the two coders reconvened to review all responses and reached a consensus on the codes for every response. We compute the Kupper-Hafner concordance (a form of inter-rater reliability for when units, i.e., responses, are coded with multiple codes) of the two independently coded sets for a total of 10 codebooks, and obtain a maximum, minimum, and average agreement of 0.76, 0.58, and 0.68, respectively, which indicates substantial agreement [23, 38, 41]. All IRR numbers are provided in Appendix D.

3.6 Limitations

We recruited participants using the Prolific crowdsourcing platform. While such platforms are popular in research studies, including other studies that solicited consumers' security and privacy perceptions for IoT devices [15, 19], they are not completely representative of the general public. In addition, in our study our participants are taking a survey and not physically visiting stores to purchase IoT products with labels. Thus, their observed behavior may not exactly match what they would do in real life, and their self-reported expected behavior may reflect biases reflective of being a study participant. Furthermore, purchase decisions in real life are likely influenced by other factors such as brand recognition, price, and functionality features. We have attempted to carefully control for these confounding factors by designing a relatively realistic scenario but using fictitious products and reminding our participants that, besides any differences illustrated on the labels,

all other functionality-related features of the devices whose labels are shown are identical.

In our study, we recruited a gender-balanced and age-balanced (in three age buckets) set of participants from the U.S. only. We believe this is appropriate as we were testing the U.S. Cyber Trust Mark and accompanying label specifically. Thus, our findings may not generalize to other IoT cybersecurity marks or labels such as those from Singapore or the E.U. [50, 51].

4 RESULTS

First, we present a summary of our participant demographics. Then, we present our results on the impact of complexity level on participants' understanding of the labels (RQ1), followed by how participants used the labels and QR codes during the study and how they would expect to use them if they encountered them on products (RQ2). Next, we present our results related to consumer preferences and attributes that would influence consumer decisions (RQ3 and RQ4). Finally, we discuss the impact of our educational intervention, age, gender, and technical literacy on consumer understanding, interactions, and preferences of labels (RQ5).

4.1 Participants

559 participants completed the survey and received compensation, with a median completion time of 12 minutes and 1 second. We filtered out responses from 41 participants according to criteria we established prior to survey distribution. As we required participants to have purchased an IoT device in the past three years, we removed 36 participants who had not done so based on their response to an open-ended pre-screen question that asked them to list the IoT devices they had purchased over the last three years (many of these participants mentioned purchasing only phones, tablets, computers, or other non-IoT devices). We removed a total of four participants based on the detection of survey straightlining, including one participant who responded with the same Likert-scale rating for all but one of the Likert-scale questions. The other three of the four participants removed for suspected straightlining responded to over 85% of Likert-scale questions with the same rating but responded to other questions in a way that clearly contradicted opinions expressed through their Likert ratings. Finally, we removed one participant who provided nonsensical responses to all three open-ended questions on the main survey.

Out of the 518 remaining participants, 176 were assigned to the low-complexity group, 172 to the medium-complexity group, and 170 to the high-complexity group. 179 participants were between the ages of 18 and 35, 177 were between the ages of 36 and 53, and 162 were age 54 or older. 30.9% of participants self-identified as having a technical background. Demographic information is shown in Table 1. To understand participants' interests in privacy and security, we asked them four questions about their security and privacy behaviors. As shown in Figure 8, most participants reported taking steps to keep their data and accounts safe, block cookies, and use two-factor authentication. However, a large percentage of participants reported that they do not typically read privacy policies.

		Low	Medium	High	Total
Age	18-35	68(13.1%)	51(9.8%)	60(11.6%)	179(34.6%)
	36-53	56(10.8%)	64(12.4%)	57(11.0%)	177(34.2%)
	54+	52(10.0%)	57(11.0%)	53(10.2%)	162(31.3%)
Gender	Male	85(16.4%)	86(16.6%)	92(17.8%)	263(50.8%)
	Female	87(16.8%)	86(16.6%)	72(13.9%)	245(47.3%)
	Non-binary	4(0.8%)	0(0.0%)	5(1.0%)	9(1.7%)
	Prefer to self describe	0(0.0%)	0(0.0%)	1(0.2%)	1(0.2%)
Back-ground	Technical	54(10.4%)	53(10.2%)	53(10.2%)	160(30.9%)
	Non-technical	122(23.6%)	119(23.0%)	117(22.6%)	358(69.1%)
Total		176(34.0%)	172(33.2%)	170(32.8%)	518(100.0%)

Table 1: Demographic distribution of participants across label complexity groups.

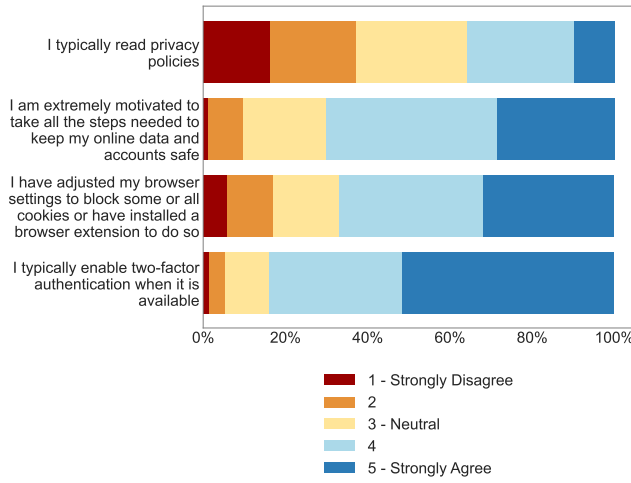


Figure 8: Q32 - How well do you agree with each of the following statements?

4.2 Understanding the Labels (RQ1)

To measure how well participants would understand and use labels, we created tasks involving label use. We first displayed three labels of the same complexity to participants, instructing them to imagine these labels were on physical product packages. Each label depicted a functionally similar smart thermostat with different security and privacy attributes (shown in Figure 6 and Figure 7), enabling controlled comparison. We asked participants which product they would be most likely to purchase after viewing the labels, followed by questions about specific information contained in the labels and overall comprehensibility/usefulness questions.

As the products were depicted as being functionally identical except for the security and privacy attributes and any differences shown on the label, we expected that participants would be most likely to select the product with the best security and privacy attributes if they had reviewed and understood the information on the medium-, high-, or ultra-high-complexity labels. When asked about which device participants would purchase, we found statistically significant differences in which option participants would select between all label groups ($p < 0.001$ between low-complexity

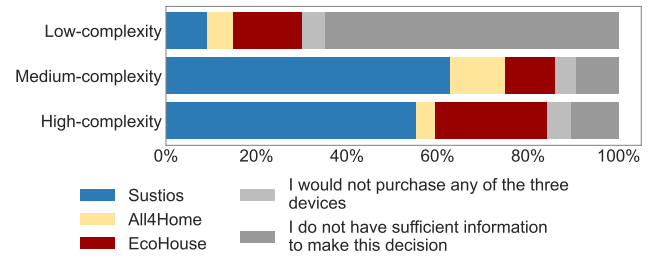


Figure 9: Q2 - Assuming that all three devices have identical functionality, which of the three devices are you most likely to purchase, given the information on the labels? Sustios has the best security and privacy attributes, followed by All4Home. EcoHouse has the worst security and privacy attributes.

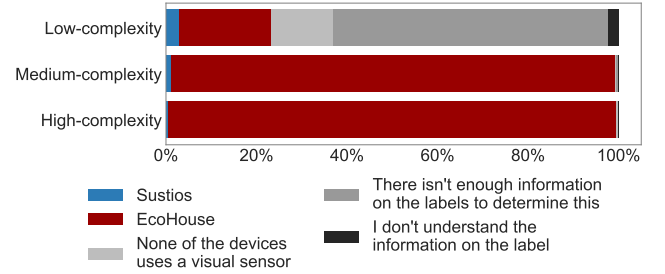


Figure 10: Q5 - Which device uses a camera or other visual sensor? The correct answer is EcoHouse.

and medium-complexity groups and between low-complexity and high-complexity groups; $p = 0.01$ between medium-complexity and high-complexity groups). As shown in Figure 9, 55.3% and 62.8% of participants in the high-complexity and medium-complexity group respectively selected Sustios, which had the best privacy and security features. 68.3% of participants in the low-complexity group said they did not have sufficient information to make the decision. While participants in the low-complexity group were not shown sufficient information on the label, they could retrieve more information through the QR code, but we observed that 67% did not scan the QR codes.

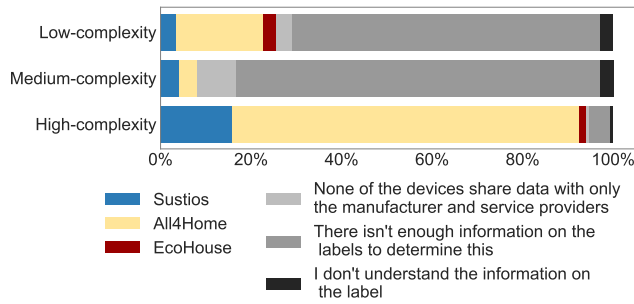


Figure 11: Q6: Which device shares data with ONLY the manufacturer and service providers? The correct answer is All4Home.

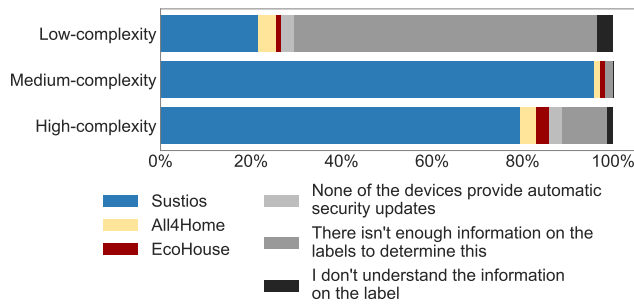


Figure 12: Q8 - Which device provides consent-based security updates? The correct answer is Sustios.

Participants were then asked to use the labels to identify which product had a particular security or privacy attribute. As shown in Figure 10, we found that 98.3% and 99.4% of medium- and high-complexity participants, respectively, were able to correctly identify the device that uses a camera or other visual sensor (Q5) compared to 24.3% of low-complexity participants ($p = 0.003$ between low and medium, and $p = 0.003$ between low and high). Similarly, as shown in Figure 12, 95.9% and 79.4% of medium- and high-complexity participants, respectively, were able to correctly select the device that provided consent-based-security updates (Q8) compared to 21.6% of low-complexity participants ($p = 0.003$ between low and medium, and $p = 0.003$ between low and high). In this case, the medium-complexity group achieved a significantly higher accuracy rate compared to the high-complexity group ($p = 0.003$). For these questions, the medium- and high-complexity package labels included the information needed to find the correct answer, while the low-complexity groups had to scan the QR codes to find the correct answer.²

In line with low-complexity results, the medium-complexity group's performance declined significantly if the security and privacy attribute in question was not shown on the medium-complexity packaging label and had to be accessed via the QR code. As shown

²There was a small typo in the answer choices for this question where participants were given the option to select "None of the devices provide automatic security updates" instead of "None of the devices provide consent-based security updates," as stated in the question. The typo had minimal impact on the results.

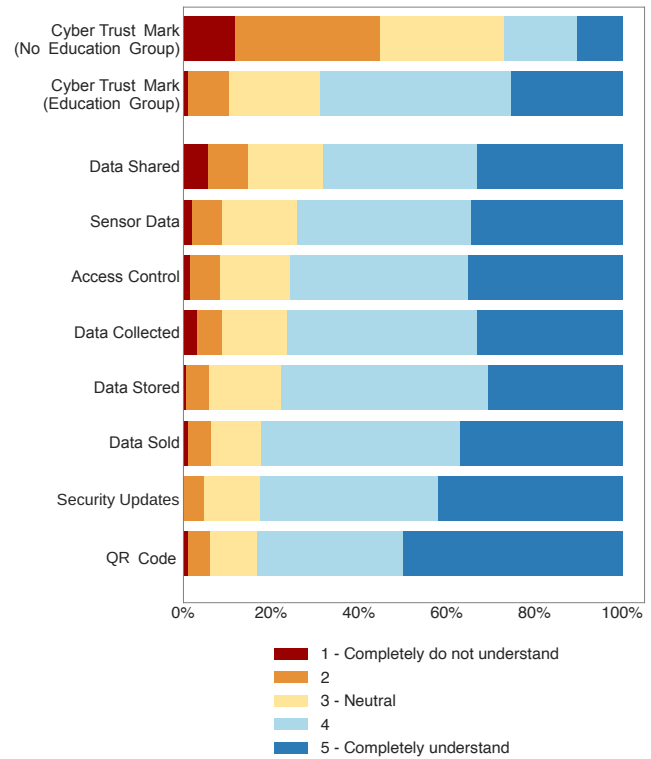


Figure 13: Q18 - How well do you feel you understand each attribute? We tested all attributes for differences between groups who did and did not receive an educational intervention and found significant differences only for the Cyber Trust Mark.

in Figure 11, less than 5% from medium-complexity correctly answered our question about who data is shared with (Q6), compared to nearly 20.6% for low-complexity ($p = 0.003$) and more than 77.4% for high-complexity ($p = 0.003$).

All of the label attributes other than the Cyber Trust Mark had been tested in prior user studies and found to be fairly well understood [15, 17]. We asked participants to self-report how well they understood each label attribute that appeared on the packaging label for their condition (Q18). This allowed us to confirm that our participants also felt they understood the attributes and to compare the understanding of the Cyber Trust Mark to the understanding of other attributes. In Figure 13, with the exception of the Cyber Trust Mark, we ranked these attributes from best to least understood. We can see that while most participants said they understood the QR code and other security and privacy attributes, fewer said they understood the Cyber Trust Mark. As will be discussed further in Section 4.5, those exposed to the educational intervention had a significantly different understanding of the Cyber Trust Mark but not the other attributes.

4.3 Consumer Behavior and Intentions (RQ2)

We used our shopping scenario and product comparison tasks to create a controlled but relatively realistic scenario to observe how

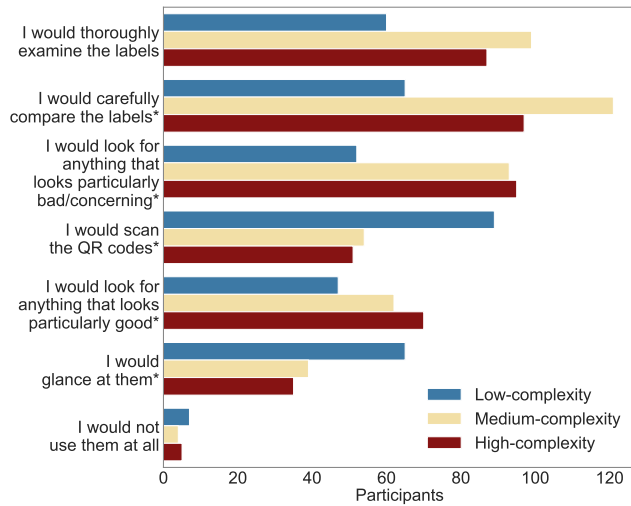


Figure 14: Q1 - If you saw these three labels on their products' packaging, would you consider them as you shop? Which of the following actions would you take? Participants saw all three labels corresponding to their assigned complexity group. An asterisk (*) indicates a statistically significant difference between label complexity groups. Complete statistical results can be found in Appendix F.

participants would likely interact with IoT package labels in the wild. We extracted data from our web server logs to observe when participants interacted with labels through QR codes (RQ2a) and asked survey questions to gain an understanding of the reasons behind participants' behavior and their self-reports of how they would likely use such labels in the future (RQ2b).

First, we asked participants whether they would consider the labels if they were shopping for a product and saw them on the packaging (Q1). As shown in Figure 14, a higher percentage of participants from the medium- and high-complexity groups responded that they would examine the information presented, including looking for anything particularly concerning ($p < 0.001$ between low and medium, and low and high), carefully comparing the labels ($p < 0.001$ between low and medium, and $p = 0.002$ between low and high), and thoroughly examining the labels ($p < 0.001$ between low and medium, and $p = 0.007$ between low and high). Participants in the low-complexity condition were most likely to say they would scan the QR code ($p = 0.003$ between low and medium, and $p = 0.001$ between low and high). For most of these options, no significant difference is found between the medium- and high-complexity groups.

Using web server log data, we calculated the percentage of participants within each complexity group that scanned different numbers of QR codes they were shown. As shown in Figure 15, 33.0% of participants in the low-complexity group scanned the QR code on at least one label, while the figure drops significantly for the medium- and high-complexity groups to 4.7% and 12.4% respectively ($p = 0.003$ between low- and medium-complexity, $p = 0.003$ between low and high, and not significant between medium and high). Among participants who scanned more than three QR codes, 13 of them were

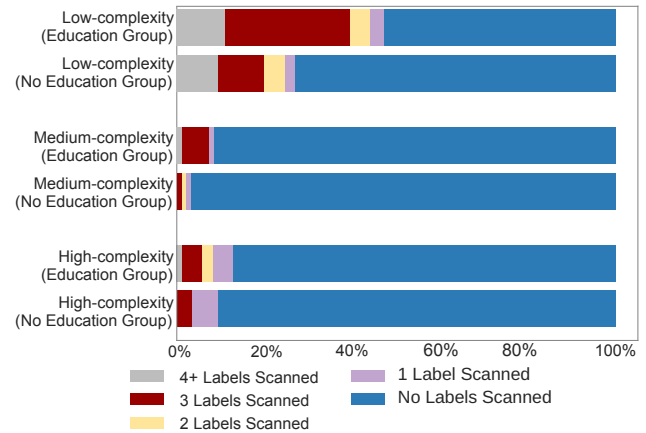


Figure 15: Number of QR codes scanned by label complexity group and groups who did and did not receive educational intervention. There were statistically significant differences between the education and no-education groups as well as between the low-complexity group with educational intervention and the low-complexity group without educational intervention.

from the low-complexity group and scanned an average of 6.8 times. These participants scanned the same QR codes more than once as they went back and forth between labels, looking for information to answer questions that those in the low-complexity group could access only through the QR codes. Likely, they did not know how to return to the previously scanned labels using the browser on their phones. Only one participant from each of the medium- and high-complexity groups scanned more than three times. We also found significant differences in the scanning behavior between the education and the no-education group, as discussed in Section 4.5.

We asked the participants who self-reported in the survey that they did not scan the QR code to identify the primary reason for not doing so (Q12). Our results, shown in Figure 16, illustrate that the most common reason was the time burden (32.7%), followed by not being interested in the information (26.4%). A large number of participants (22.8%) were also worried that scanning QR codes could be insecure, which is a realistic threat [49].

We asked participants how likely they would be to scan a QR code for more information if they saw a label when actually shopping for a device (Q10). Across all conditions, 44.4% of participants said they were likely or very likely to scan the QR code. There were no significant differences between conditions.

We asked our participants what they would likely do to get more information if they were in a store and saw the label of their assigned complexity level with a QR code on the packaging (Q11). Across all groups, about half said they would scan the QR code (49.6%). Others said they would search online (35.1%) or visit the manufacturer's websites (7.1%). There were no significant differences found between complexity groups.

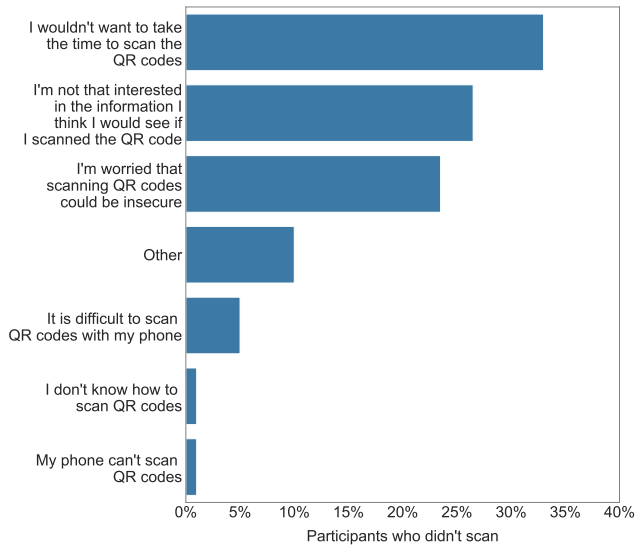


Figure 16: Q12 - Which of the following best describes why you wouldn't be likely to scan the QR code? This question was only shown to participants who did not scan the QR code.

4.4 Consumer Preferences (RQ3 and RQ4)

We asked participants a series of questions about their opinions about the specific label they viewed. Additionally, if the participant scanned the QR code, we asked them a series of questions related to the retrieved label. We included open-ended questions that elicit participants' opinions on labels they saw and ideas for potential improvements.

We first asked the participants which attributes on the label would most influence their decision to purchase the IoT device (Q20). The influence ratings, shown in Figure 17, highlight that participants found privacy attributes (such as whether the data was sold to third parties, shared, stored, or collected) as well as security attributes (including security updates and access control) to be influential to their purchase decision. Again, the only attribute to which education makes a difference is the Cyber Trust Mark, which we will further discuss in Section 4.5.

Similar to our results for understanding, the QR code and the Trust Mark were reported to be the two least influential elements. Note that we did not ask participants to explicitly compare a device with a Cyber Trust Mark (indicating compliance with baseline standards) to a device without one (indicating lack of compliance). Thus, we cannot assess the influence of the Trust Mark in consumers' decision-making between devices with and without a Trust Mark.

As shown in Figure 18, when we asked participants how helpful they found the information on the packaging label (Q22), 68.6% of participants from the medium-complexity group and 78.8% from the high-complexity group found the information presented somewhat or extremely helpful, while a significantly lower percentage (17.1%) from the low-complexity group found it helpful ($p < 0.001$ for all three pairwise tests).

To better understand participants' preference for label complexity, we asked them whether the package label they were shown

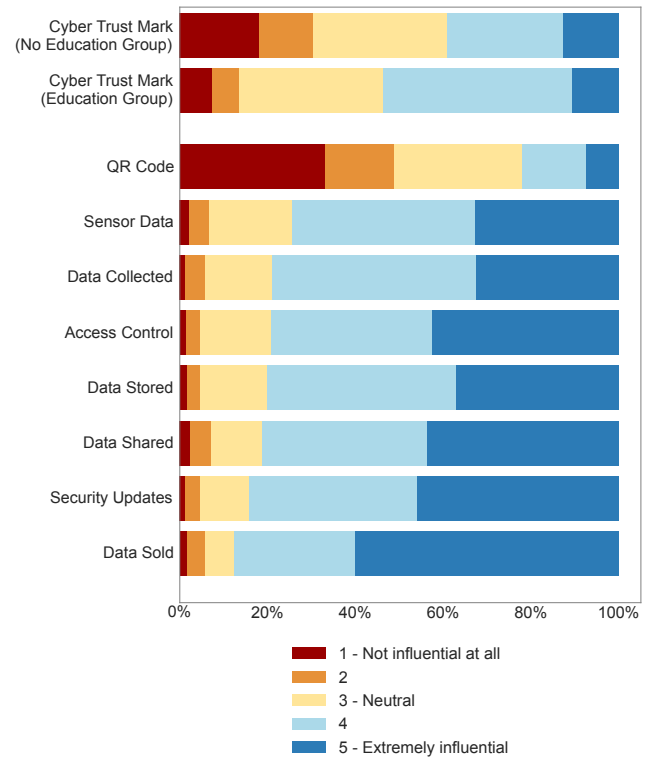


Figure 17: Q20 - How much does each of the attributes influence your purchase decision? We tested all attributes for differences between educational groups and found significant differences only for the Cyber Trust Mark.

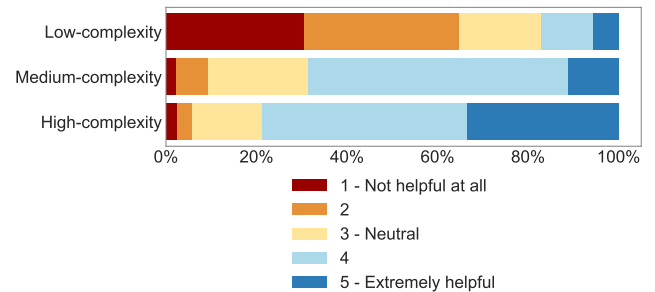


Figure 18: Q22 - Overall, how helpful would you find the information on the label shown above when making a purchasing decision?

had enough information, too much information, or just about the right amount (Q24). As shown in Figure 19, we found that only 15.3% of the participants in the low-complexity group found the level of information just right, with 80.1% reporting the level of information is not enough. In contrast, for the medium- and high-complexity labels, participants reported them being just right in terms of information presented 51.2% and 78.8% of the time, respectively, far exceeding ($p = 0.003$ between low and medium, and $p = 0.003$ between low and high) the low-complexity group. The

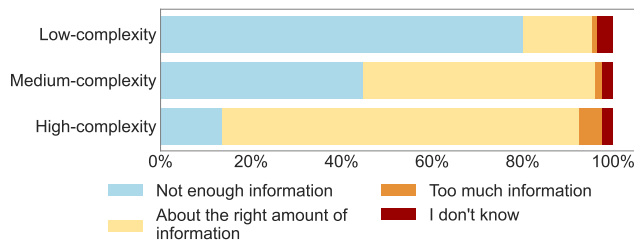


Figure 19: Q24 - What do you think about the amount of information on the labels you were shown above?

high-complexity group also had a significantly higher percentage of participants who said the label shown to them contained the right amount of information ($p = 0.003$).

Notably, only a small percentage of participants from any condition thought that there was too much information: 5.3% from the high-complexity group and less than 2% from low- and medium-complexity groups.

We also asked participants what additional information they would like to see on the labels in an open-ended question (Q27). In every condition, a large number of people remarked that they wanted the label to contain more information. 63.6% of participants in the low-complexity condition remarked that they wanted more information, and some mentioned specifically wanting more actual information on the packaging label without having to scan a QR code. One commented, “The details should be directly on the label. No business should expect a customer to scan some random QR code.” Another participant wrote, “Any information on security and privacy would help. This doesn’t give much info.” The only specific information that participants frequently requested was more information about the types of data shared (requested by 42.0% of participants from the medium-complexity and 16.0% of participants from the low-complexity groups who did not scan). One participant from the medium-complexity group stated, “I need more clarification about who it shares the information with directly on the label.” Note that those in the medium-complexity group would have seen a list of the types of information shared, but with no details about the sharing, whereas those in the low-complexity group who did not scan would not have seen any mention of sharing. Participants from the high-complexity group were more likely to be satisfied with the amount of information on the label. One wrote, “There is already a lot of information on the label, I wouldn’t want to add anymore because it’d feel like too much info.”

Since the labels include a QR code, we followed up with another question where we asked participants to rate the level of information they saw *after* scanning the QR code (Q25). This question was only asked of participants who indicated that they had scanned the QR code. Across all three conditions, an overwhelming majority reported that the secondary layer label that was shown had the right amount of information (72.9%, 81.8%, and 76.9% of low-, medium-, and high-complexity group participants with no statistically significant difference between conditions). Nonetheless, a small percentage of participants still reported not having enough information, and a few (< 8%) thought the secondary layer contained too much information.

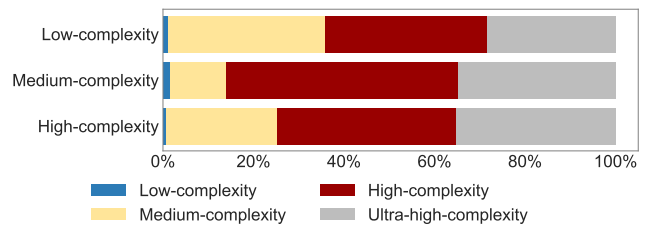


Figure 20: Q28 - When you are shopping for an IoT device, which of the four label designs above would you be most interested in seeing on the product packaging? Participants saw label 1, 2, 3, and 4 as options, which correspond to low-, medium-, high-, and ultra-high-complexity label.

After responding to all questions related to their assigned label, participants were shown four labels: the low-, medium-, and high-complexity labels, as well as the ultra-high-complexity label shown to participants who scanned the QR code or clicked the button on the high-complexity label. Participants were then asked to select the label they would most like to see on product packaging (Q28). As shown in Figure 20, participants overwhelmingly did not want to see the low-complexity label: only 6 out of 518 respondents selected it as their top choice. The most popular option was the high-complexity label, which was selected by 42.1% of participants across all conditions, followed by the ultra-high-complexity label at 32.8%, with the medium- and low-complexity label accounting for the remaining 23.9% and 1.16% respectively. Interestingly, those in the medium-complexity group were less interested in seeing the medium-complexity label than those in the other two groups ($p = 0.003$ between low and medium, and $p = 0.031$ between medium and high), perhaps because they had experienced using it and were more aware of its limitations.

We followed up with a question asking participants to explain the reasons behind their label choice (Q29). 46.4% of participants who chose the medium-complexity label and 53.7% of participants who chose the high-complexity label mentioned the amount of information as one of their reasons. Many participants considered the medium-complexity label a good balance between too little and too much information. One participant who chose the medium-complexity label stated, “I feel like it has a good amount of basic information to go off of. If I needed more, I would look it up online. The [low] felt like it had almost no information, and [high] and [ultra-high] felt like information overload.” Participants who selected the high-complexity label shared similar views while also complimenting the high-complexity label for presenting up-front information without having to scan the QR code. One participant added “it’s a lot faster for me to read the label that is already there, as opposed to scanning a QR code. Also I am a little wary of scanning random QR codes unless I already know that I can trust the source, as I have heard about malicious QR codes.” More than 80% of the participants who chose the ultra-high-complexity label said they preferred the label because it contained a lot of information. One of these participants added, “It has the most detailed information. I almost picked label [high] but label [ultra-high] had some of the information that I was looking for that label [high] did not have.”

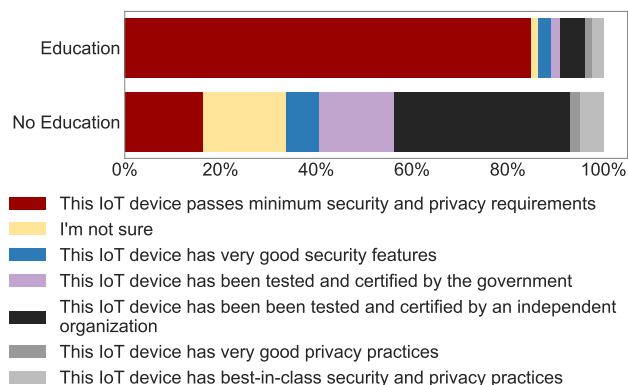


Figure 21: Q4: - Which of the following do you think best describes what the presence of the Cyber Trust Mark on the label represents? The correct answer is “This IoT device passes minimum security and privacy requirements.”

We asked participants for potential improvements to the label that was shown to them throughout the survey. For the low-complexity group, about a third of participants asked about what the Cyber Trust Mark means and wanted a clearer explanation regarding what “more info” entails, such that they know what they are expecting to see after scanning the QR code. 24.0% of participants who saw the low-complexity label indicated wanting the label to contain at least some basic information without having to scan the QR code. According to one participant, “I want more information on the label itself. Many people do not know how to use QR codes, or do not have the technology or experience to use it.”

Participants from the medium-complexity group were specifically interested in knowing more about shared or sold data, with nearly 30% of them explicitly asking for that information to be presented on the package label. In addition, 17.4% of medium-complexity participants asked for more security/privacy-related information, and 19.8% asked for more information generally. For participants from the high-complexity group, fewer mentioned wanting more information of any kind, and 8.8% of them said they wanted to reduce the amount of content on the label. One of them stated, “it feels very busy. I don’t know where to look. It should be like amazon or youtube where you know where the information is on the page. Perhaps remove sensor type. We know microphones capture sound. Prioritize shared with, sold to, data stored on cloud. Put everything else in the qr code.” Across all conditions, participants had minor design suggestions related to fonts, color, layout, and other design features.

Next, we presented participants with the same four label layers and asked which they would like to see after scanning the QR Code (Q30). The ultra-high-complexity label was selected by 48.8% of participants across all groups, followed by the high-complexity label selected by 35.1% of all participants. The responses had no significant differences between complexity groups.

The new US cybersecurity certification and labeling program is designed to help Americans more easily choose smart devices that are safer and less vulnerable to cyberattacks. Products that include the “U.S. Cyber Trust Mark”, pictured below, on their packaging or website meet baseline standards for cyber security and privacy. You can scan the accompanying QR code to get more information about the product’s security and privacy attributes.



U.S. CYBER TRUST MARK

Figure 22: The brief educational intervention was randomly shown to half of the participants.

4.5 U.S. Cyber Trust Mark Education (RQ5a)

Existing labeling programs, such as the Energy Star label for energy efficiency, were supported with extensive education campaigns to help consumers know what to look for when purchasing appliances [54]. As the U.S. Cyber Trust Mark is not yet available on packages, consumers are not yet familiar with its purpose and meaning. We developed a simple educational intervention (shown in Figure 22) to explain the purpose of the U.S. Cyber Trust Mark and QR code and showed it to half our participants across all label groups. We did not allow them to proceed further in the study until they correctly answered questions to confirm they had a basic understanding of the Trust Mark and QR code. We asked these questions again to all participants later in the survey and compared the accuracy rate of participants who received the educational intervention with those who did not. Further, we examined whether the educational intervention impacted whether participants scanned the QR codes, their expectation of what they would see if they scanned the QR codes, their self-reported understanding of the Trust Mark, and their self-reported assessment of the Trust Mark’s influence on their purchase decisions.

After answering three survey questions, all participants, regardless of educational interventions, were shown the question about the purpose of the Cyber Trust Mark (Q4). Participants in the education group significantly outperformed those in the no-education group across all three label complexities. As shown in Figure 21, 84.8% of all participants in the education group selected the correct option, which was that the presence of the mark meant that the device met baseline security and privacy requirements, as compared to only 16.5% in the no-education group ($p = 0.003$). Over half the participants in the no-education group incorrectly believed that the mark indicated that the device had been tested and certified by an independent organization or the government.

We used web server log data to analyze whether education affected the number of QR codes participants scanned (shown in

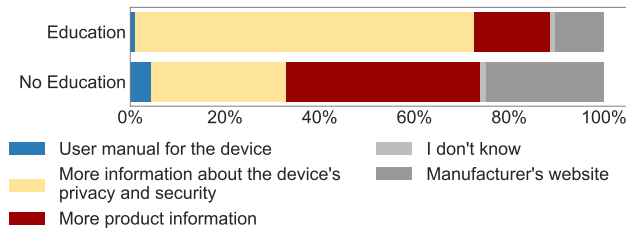


Figure 23: Q13 - Which of the following best describes what you would expect to find after scanning the QR code? Only those who did not scan were asked this question. The correct response is “More information about the device’s privacy and security.”

Figure 15). We found that across all participants, those in the education group were significantly more likely to scan the QR code more times ($p = 0.012$) than those in the no-education group. Participants in the education group scanned an average of 0.813 times, while those in the no-education group scanned an average of 0.276 times, a nearly three-fold increase. Moreover, we examined the effect of education within each complexity group, finding a significant difference only for the low-complexity group ($p = 0.003$),³ with 23.7% of education-group low-complexity participants scanning at least once compared to 11.1% of non-education-group low-complexity participants.

During the latter half of the survey, participants who did not scan the QR code were asked what information they expected to see after scanning the QR code (Q13). The results shown in Figure 23 indicate that more participants in the education group answered the question correctly 71.7% as compared to those who did not receive the education (28.6%, $p = 0.003$). We found no statistically significant relationships across complexities for both of these questions.

As discussed in previous sections, we asked participants to rate their level of understanding of each label attribute and the extent to which these attributes would influence their purchase decisions (Figures 13, 17). We found participants who were exposed to education on the Cyber Trust Mark indicated having a better understanding of the Trust Mark ($p < 0.001$), with an average Likert rating of 3.82 on a 1-5 scale compared to 2.8 for the no-education group. Those in the education group also rated the Trust Mark as having more influence on their purchasing decision ($p = 0.003$).

4.6 Effects of Demographic Factors (RQ5b, RQ5c, and RQ5d)

In the prescreening survey, we asked participants to report whether they had any education or experience in engineering, computer science, or similar technical fields to evaluate the impact of technical backgrounds on survey responses. For the vast majority of the questions, we found no statistically significant difference between participants with or without a technical background in label

³We also see differences in average numbers of scans between education groups within medium- and high-complexity groups (see 15). However, our non-parametric tests (Kruskal-Wallis test and Mann-Whitney U test) likely lack the power to find a statistical difference in low scan counts.

comprehension, label preference, and scanning behavior. We found that the only significant differences to arise were that participants with a technical background reported a higher tendency to read privacy policies (an average of 3.24 on a scale of 1 to 5 compared to 2.78 for those without technical experience, $p < 0.001$) and a greater motivation to keep their online data and accounts safe (4.08 and 3.78 for participants with and without technical experience respectively, $p = 0.012$). These results suggest that our label designs work similarly regardless of technical background.

We tested whether age is a determining factor in label comprehension, label preference, and consumer behavior. We found that young people aged 18-35 were less willing to scan QR codes compared to the other two age groups. On a scale of 1 to 5, the mean Likert score of willingness to scan for 18-35 age group is 2.7, compared to 3.23 for 36-53 age group and 3.37 for 54+ age group ($p = 0.003$ between 18-35 and 36-53, and $p < 0.001$ between 18-35 and 54+ age groups). Participants aged 18-35 were also reported to be less likely to take privacy-related actions, including reading privacy policies (2.61 for participants aged 18-35 compared to 3.19 for those aged 36-53, and 2.96 for ages 54+, $p < 0.001$) and less motivated to take steps to ensure online privacy (3.64 for 18-35 compared to 4.09 for 36-53 and 3.9 for 54+, $p < 0.001$). When asked about which label they prefer, our results showed that young people differ significantly from other age groups ($p = 0.005$), preferring the medium-complexity label more than people in the 36-53 and the 54+ age groups (33.0%, 18.1%, and 20.4% of the groups, respectively), with a larger percentage of people in the latter two groups preferring the high- or ultra-high-complexity labels (66.5%, 79.1%, and 79.6% of the groups, respectively). In addition, we found several numerically small but statistically significant differences between age groups for some survey questions without clear trends in either direction.

Based on participants’ responses in the prescreening survey, we divided participants into male and non-male groups and tested for the impact of gender differences concerning RQ1, RQ2, RQ3, and RQ4. We found no significant differences between the two groups.

5 DISCUSSION

Our results demonstrate that IoT purchasers are interested in learning more about the security and privacy of devices and they would like to see this information on product packaging. As detailed below, our participants had a strong preference for higher complexity labels and were almost unanimously unsatisfied with the low-complexity label. We found that our participants disliked accessing critical information by QR codes, and we observed that comparing labels on a phone screen is awkward. Without education, we found substantial confusion about the Trust Mark and QR code. Our simple educational intervention improved understanding of the QR code’s purpose but had a relatively modest effect on QR code scanning. Finally, our results support the need for including privacy information along with security information on package labels. As the U.S. FCC defines requirements for using the U.S. Cyber Trust Mark and considers designs for accompanying IoT labels, the CISPL label (which we used for our high-complexity label) [57] or a simplified version, similar to the medium-complexity label we tested, presents a deployable baseline that can be refined as

new requirements are articulated. However, as label designs evolve, further testing is critical to ensure labels meet consumer needs.

Strong preference for higher complexity. Study participants in all label conditions were overwhelmingly opposed to the low-complexity label that required scanning a QR code in order to obtain any security or privacy information. Indeed, only 6 out of 518 participants indicated they most preferred the low-complexity label. Most preferred to see the high-complexity label on product packaging, although some preferred the ultra-high-complexity label and some preferred the simpler medium-complexity label. In general, participants preferred more information, regardless of which label they were shown, educational intervention, their age, or whether they had a technical background.

The medium- and high-complexity labels performed similarly, although there are some tradeoffs between them. The high-complexity label was more often preferred by participants and contained more information that might be needed to compare products, but participants made fewer comparison errors using the medium-complexity label. Both types of labels might be offered as options for manufacturers to use depending on available space on product packaging.

Usability issues with QR codes. While more participants scanned the QR code in our low-complexity condition when they could not obtain any information otherwise, most did not scan and said they would be reluctant to do so in the future. Some mentioned the inconvenience of scanning, while others were concerned that QR codes might not be secure. We note that even if participants were to scan QR codes, comparing labels on a small phone screen is difficult and would likely require going back and forth between labels and re-scanning multiple times—something we observed several participants doing. Emami-Naeini et al. have proposed a comparison tool that could produce a compact table for consumers comparing a small number of devices against their preferred criteria [16]. While such a tool would make it easier for consumers to compare labels on a phone, it would still be useful to have the information directly on the product packaging. Indeed, consumers are used to seeing food nutrition labels, light bulb energy labels, and other consumer labels on packages, allowing easy side-by-side comparison.

Education is Key. As it is infeasible to fit all possible privacy and security information on a physical label while also keeping it up to date, a QR code (or a URL) is required to link more comprehensive labels for users, regulators, or experts. However, as we've found, simple linkage isn't enough. Consumers will need to be educated about what the U.S. Trust Mark implies, and how scanning the QR code leads to more security and privacy information about products, ultimately leading to better-informed purchase decisions. Wording improvements on the label or the Trust Mark might improve clarity and serve to nudge people to scan label QR codes. Furthermore, in-store signage (e.g., on store shelves) next to IoT products might help educate consumers. Prior efforts such as the Energy Star and Energy Guide Labels were supported by multi-year educational campaigns to inform consumers. IoT labels are arguably more complex and might require even larger investments in education. Encouragingly, we show that our educational intervention improved the understanding of the Trust Mark and what consumers could find upon scanning the QR code. This understanding also translated to behavior; we saw a modest increase in

the number of participants who scanned the QR codes, particularly in the low-complexity condition. However, to a large extent, most participants were still not motivated to scan the QR code, regardless of educational intervention.

Security and Privacy. Participants were interested in seeing a range of privacy and security attributes on the label, and seemed especially interested in privacy-related attributes that would inform them about what data would be collected, utilized, and shared. This is particularly important since the criteria that the NIST IR 8425 document [47] lists as the “baseline criteria” that may drive the requirements to get the Cyber Trust Mark are mostly security-focused, with no explicit mention of privacy factors. Based on our study and similar findings in prior work [15, 16], privacy factors such as which sensors devices have, whether data is sold, and how it will be used are critical to include on the package label itself. Furthermore, privacy information may be essential for the U.S. label to be recognized internationally, given that several countries are basing their own requirements around the ETSI 303645 standard [10] which explicitly discusses privacy factors.

6 CONCLUSION

We studied the effectiveness of high-, medium-, and low-complexity versions of an IoT security and privacy label designed for product packaging. Each version included the newly introduced U.S. Cyber Trust Mark and a QR code with the medium- and high-complexity versions including additional security and privacy information. We conducted a 518-participant online study in which participants were randomly assigned a label complexity level and asked to use the labels to compare three functionally similar smart thermostats. Half the participants received a brief educational intervention at the beginning of the study, informing them about the purpose of the U.S. Cyber Trust Mark and accompanying QR code. At the end of the study, participants were shown labels of all three complexity levels along with an ultra-high-complexity label. We investigated the impact of label complexity level on consumers' understanding of label information, interactions with labels, and preferences for the labels. In addition, we investigated which label attributes were most influential. Finally, we explored the impact of the brief educational intervention, age, gender, and technical background on understanding, interactions, and preferences. Our findings show that participants strongly favored the higher-complexity labels and were reluctant to scan the QR codes, regardless of age, gender, or technical background. They reported finding a range of privacy and security attributes influential. While our educational intervention improved understanding of the purpose of the Trust Mark and QR code, our results suggest that it had only a small impact on motivation to scan the QR code.

ACKNOWLEDGMENTS

This research was funded in part by Craig Newmark Philanthropies and the National Science Foundation award SaTC-1801472. The authors are grateful to Omer Akgul for his assistance with data analysis and paper revisions.

REFERENCES

- [1] Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J Alex Halderman, Luca Invernizzi, Michalis

- Kallitsis, et al. 2017. Understanding the mirai botnet. In *26th USENIX security symposium (USENIX Security 17)*, 1093–1110.
- [2] Abeer Assiri and Haya Almagwashi. 2018. IoT security and privacy issues. In *2018 1st International Conference on Computer Applications & Information Security (ICCAIS)*. IEEE, 1–5.
- [3] Consumer Technology Association. 2023. Consumer Technology Association joins White House to support cybersecurity labeling program to protect consumers from IoT attacks. <https://www.cta.tech/Resources/Newsroom/Media-Releases/2023/July/CTA-Joins-White-House-IoT-Labeling-Program>
- [4] Hany F Atlam and Gary B Wills. 2020. IoT security, privacy, safety and ethics. *Digital twin technologies and smart cities* (2020), 123–149.
- [5] Yoav Benjamini and Yosef Hochberg. 1995. Controlling the false discovery rate: a practical and powerful approach to multiple testing. *Journal of the Royal statistical society: series B (Methodological)* 57, 1 (1995), 289–300.
- [6] Poornima M Chanal and Mahabaleswar S Kakkasageri. 2020. Security and privacy in IoT: a survey. *Wireless Personal Communications* 115, 2 (2020), 1667–1693.
- [7] Federal Communications Commission. 2023. <https://www.fcc.gov/cybersecurity-certification-mark>
- [8] Federal Communications Commission. 2023. FCC proposes cybersecurity labeling program for Smart Devices. <https://www.fcc.gov/document/fcc-proposes-cybersecurity-labeling-program-smart-device>
- [9] Lorrie Faith Cranor. 2022. Mobile-app privacy nutrition labels missing key ingredients for success. *Commun. ACM* 65, 11 (2022), 26–28.
- [10] Technical Committee Cyber Security (CYBER). 2020. Cyber Security for Consumer Internet of Things: Baseline Requirements. (2020). https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf
- [11] Mehri Dabbagh and Ammar Rayes. 2019. Internet of things security and privacy. *Internet of Things from hype to reality* 621 (2019), 211–238.
- [12] Marc Dupuis and Mercy Ebenezer. 2018. Help wanted: Consumer privacy behavior and smart home internet of things (iot) devices. In *Proceedings of the 19th Annual SIG Conference on Information Technology Education*. 117–122.
- [13] Serge Egelman and Eyal Peer. 2015. Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (Seoul, Republic of Korea) (CHI '15). Association for Computing Machinery, New York, NY, USA, 2873–2882. <https://doi.org/10.1145/2702123.2702249>
- [14] Pardis Emami-Naeini, Yuvraj Agarwal, and Lorrie Faith Cranor. 2021. Specification for CMU IoT security and privacy label. *Privacy_and_Security_Specifications.pdf* (2021).
- [15] Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, and Hanan Hibshi. 2020. Ask the experts: What should be on an IoT privacy and security label?. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 447–464.
- [16] Pardis Emami-Naeini, Janarth Dheendhayan, Yuvraj Agarwal, and Lorrie Faith Cranor. 2021. An informative security and privacy “nutrition” label for internet of things devices. *IEEE Security & Privacy* 20, 2 (2021), 31–39.
- [17] Pardis Emami-Naeini, Janarth Dheendhayan, Yuvraj Agarwal, and Lorrie Faith Cranor. 2021. Which privacy and security attributes most impact consumers’ risk perception and willingness to purchase IoT devices?. In *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 519–536.
- [18] Pardis Emami-Naeini, Janarth Dheendhayan, Yuvraj Agarwal, and Lorrie Faith Cranor. 2023. Are Consumers Willing to Pay for Security and Privacy of IoT Devices?. In *In Proceedings of the 32nd USENIX Security Symposium*.
- [19] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. 2019. Exploring how privacy and security factor into IoT device purchase behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–12.
- [20] Cori Faklaris, Laura A. Dabbish, and Jason I. Hong. 2019. A Self-Report Measure of End-User Security Attitudes (SA-6). In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, Santa Clara, CA, 61–77. <https://www.usenix.org/conference/soups2019/presentation/faklaris>
- [21] Ronald Aylmer Fisher. 1970. Statistical methods for research workers. In *Breakthroughs in statistics: Methodology and distribution*. Springer, 66–70.
- [22] Nadine Guhr, Oliver Werth, Philip Peter Hermann Blacha, and Michael H Breitner. 2020. Privacy concerns in the smart home context. *SN Applied Sciences* 2 (2020), 1–12.
- [23] Marian Harbach, Alexander De Luca, Nathan Malkin, and Serge Egelman. 2016. Keep on lockin’ in the free world: A multi-national comparison of smartphone locking. In *Proceedings of the 2016 chi conference on human factors in computing systems*. 4823–4827.
- [24] Stephen Herwig, Katura Harvey, George Hughey, Richard Roberts, and Dave Levin. 2019. Measurement and analysis of Hajime, a peer-to-peer IoT botnet. In *Network and Distributed Systems Security (NDSS) Symposium*.
- [25] The White House. 2021. Executive Order on Improving the Nation’s Cybersecurity. <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>
- [26] The White House. 2022. Statement by NSC Spokesperson Adrienne Watson on the Biden-Harris Administration’s Effort to Secure Household Internet-Enabled Devices. <https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/20/statement-by-nsc-spokesperson-adrienne-watson-on-the-biden-harris-administrations-effort-to-secure-household-internet-enabled-devices/>
- [27] The White House. 2023. Biden-Harris Administration Announces Cybersecurity Labeling Program for Smart Devices to Protect American Consumers. <https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/18/biden-harris-administration-announces-cybersecurity-labeling-program-for-smart-devices-to-protect-american-consumers/>
- [28] Yong Ho Hwang. 2015. IoT security & privacy: threats and challenges. In *Proceedings of the 1st ACM workshop on IoT privacy, trust, and security*. 1–1.
- [29] Esther DT Jaspers and Erika Pearson. 2022. Consumers’ acceptance of domestic Internet-of-Things: The role of trust and privacy concerns. *Journal of Business Research* 142 (2022), 255–265.
- [30] Aqsa Kashaf, Vyas Sekar, and Yuvraj Agarwal. 2020. Analyzing third party service dependencies in modern web services: Have we learned from the mirai-dyn incident?. In *Proceedings of the ACM Internet Measurement Conference*. 634–647.
- [31] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W Reeder. 2009. A “nutrition label” for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security*. 1–12.
- [32] Patrick Gage Kelley, Lucian Cesca, Joanna Bresee, and Lorrie Faith Cranor. 2010. Standardizing privacy notices: an online study of the nutrition label approach. In *Proceedings of the SIGCHI Conference on Human factors in Computing Systems*. 1573–1582.
- [33] Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. 2013. Privacy as part of the app decision-making process. In *Proceedings of the SIGCHI conference on human factors in computing systems*. 3393–3402.
- [34] Hae-Young Kim. 2017. Statistical notes for clinical researchers: Chi-squared test and Fisher’s exact test. *Restorative dentistry & endodontics* 42, 2 (2017), 152–155.
- [35] Simon Koch, Malte Wessels, Benjamin Altpeter, Madita Olvermann, and Martin Johns. 2022. Keeping privacy labels honest. *Proceedings on Privacy Enhancing Technologies* 4, 486–506 (2022), 2–2.
- [36] William H Kruskal and W Allen Wallis. 1952. Use of ranks in one-criterion variance analysis. *Journal of the American statistical Association* 47, 260 (1952), 583–621.
- [37] J Sathish Kumar and Dhiren R Patel. 2014. A survey on internet of things: Security and privacy issues. *International Journal of Computer Applications* 90, 11 (2014).
- [38] Lawrence L Kupper and Kerry B Hafner. 1989. How appropriate are popular sample size formulas? *The American Statistician* 43, 2 (1989), 101–105.
- [39] Tianshi Li, Kayla Reiman, Yuvraj Agarwal, Lorrie Faith Cranor, and Jason I Hong. 2022. Understanding challenges for developers to create accurate privacy nutrition labels. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. 1–24.
- [40] Yanzi Lin, Jaideep Juneja, Eleanor Birrell, and Lorrie Faith Cranor. 2024. Data Safety vs. App Privacy: Comparing the Usability of Android and iOS Privacy Labels. *Proceedings on Privacy Enhancing Technologies* 2024, 2 (2024).
- [41] Nathan Malkin, Alan F. Luo, Julio Poveda, and Michelle L. Mazurek. 2023. Optimistic Access Control for the Smart Home. In *2023 IEEE Symposium on Security and Privacy (SP)*.
- [42] Marie-Helen Maras. 2015. Internet of Things: security and privacy implications. *International Data Privacy Law* 5, 2 (2015), 99.
- [43] Katerina N Megias, Michael Fagan, Jeffrey Marron, Paul Watrobski, and Barbara Bell Cuthill. 2022. Profile of the IoT Core Baseline for Consumer IoT Products. (2022).
- [44] Philip Menard and Gregory J Bott. 2020. Analyzing IOT users’ mobile device privacy concerns: Extracting privacy permissions using a disclosure experiment. *Computers & Security* 95 (2020), 101856.
- [45] Cyber Security Agency of Singapore. 2021. Cybersecurity Certification Guide. (2021). https://www.csa.gov.sg/docs/default-source/our-programmes/certification-and-labelling-scheme/cls/publications/csa-cybersecurity-certification-guide.pdf?sfvrsn=a486afd5_0
- [46] Cyber Security Agency of Singapore. 2022. Cybersecurity labelling scheme (CLS). <https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme>
- [47] National Institute of Standards and Technology. 2022. *Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products*. Technical Report. U.S. Department of Commerce, Washington, D.C. <https://doi.org/10.6028/nist.cswp.02042022-2>
- [48] Karl Pearson. 1900. X. On the criterion that a given system of deviations from the probable in the case of a correlated system of variables is such that it can be reasonably supposed to have arisen from random sampling. *The London, Edinburgh, & Dublin Philosophical Magazine and Journal of Science* 50, 302 (July 1900), 157–175. <https://doi.org/10.1080/14786440009463897>
- [49] Alvaro Puig. 2023. Scammers hide harmful links in QR codes to steal your information. <https://consumer.ftc.gov/consumer-alerts/2023/12/scammers-hide-harmful-links-qr-codes-steal-your-information>
- [50] Alexandr Railean and Delphine Reinhardt. 2018. 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* (Barcelona, Spain) (*MobileHCI '18*). Association for Computing Machinery, New York, NY, USA, 103–110. <https://doi.org/10.1145/3236112.3236126>
- [51] Alexandr Railean and Delphine Reinhardt. 2021. 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, 229–245.
 - [52] Shim Sangmin. 2015. <https://davidshimjs.github.io/qrcodejs/>
 - [53] Science Senate Committee on Commerce and Transportation. 2023. S.90 - Informing Consumers about Smart Devices Act. <https://www.congress.gov/bill/118th-congress/senate-bill/90/text>, as of March 14, 2024.
 - [54] Energy Star. [n. d.]. <https://www.energystar.gov/products/how-product-earns-energy-star-label>
 - [55] Finnish Transport and Communications Agency. 2022. Cybersecurity label. <https://tietoturvamerkki.fi/en/cybersecurity-label#:~:text=The%20label%20is%20granted%20to,smart%20bracelets%20and%20home%20routers>.
 - [56] European Union. 2023. Cyber Resilience Act - Questions and Answers. https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_5375
 - [57] Carnegie Mellon University. 2021. https://iotsecurityprivacy.org/downloads/Privacy_and_Security_Specifications.pdf
 - [58] Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie Li, and Hongbin Zhao. 2017. A survey on security and privacy issues in Internet-of-Things. *IEEE Internet of things Journal* 4, 5 (2017), 1250–1258.
 - [59] Tianlong Yu, Vyas Sekar, Srinivasan Seshan, Yuvraj Agarwal, and Chenren Xu. 2015. Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the internet-of-things. In *Proceedings of the 14th ACM Workshop on Hot Topics in Networks*. 1–7.
 - [60] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End user security and privacy concerns with smart homes. In *thirteenth symposium on usable privacy and security (SOUPS 2017)*. 65–80.
 - [61] Shikun Zhang, Yuanyuan Feng, Yaxing Yao, Lorrie Faith Cranor, and Norman M. Sadeh. 2022. How Usable Are iOS App Privacy Labels? *Proc. Priv. Enhancing Technol.* 2022 (2022), 204–228. <https://doi.org/10.56553/popets-2022-0106>

A SURVEY QUESTIONS

A.1 Consent form and screening questions

This survey is part of a research study conducted by Dillon Shu at Carnegie Mellon University and is funded by Carnegie Mellon University.

A.1.1 Summary and Purpose. This is a survey about IoT device purchasing. Our study aims to figure out what information is most useful to consumers in order to help them make the most educated purchase. If you're concerned about security or privacy when purchasing IoT products, our research hopes to help improve your purchasing experience in the future.

A.1.2 Procedures. You will be provided a link to an online survey using Qualtrics. We expect this survey to take no more than 25 minutes. When filling out the survey, do NOT disclose any private or personally identifiable information about yourself or anyone else. Following the completion of the survey, you will be given a link to click as proof of completion of the survey within Prolific. Please note that this is necessary for payment.

A.1.3 Participant Requirements. Participation in this study is limited to individuals age 18 and older who live in the United States who have purchased at least 1 IoT device over the last 3 years who have also taken the screening survey.

A.1.4 Risks. The risks and discomfort associated with participation in this study are no greater than those ordinarily encountered in daily life or during other online activities.

A.1.5 Benefits. There may be no personal benefit from your participation in the study but the knowledge received may be of value to humanity.

A.1.6 Compensation & Costs. You will be compensated \$5 USD[\$0.5 for the pre-screen survey] following the completion of the survey. No payment will be given if you do not complete the study. There will be no cost to you if you participate in this study.

A.1.7 Future Use of Information. In the future, once we have removed all identifiable information from your data, we may use the data for our future research studies, or we may distribute the data to other researchers for their research studies. We would do this without getting additional informed consent from you (or your legally authorized representative). Sharing of data with other researchers will only be done in such a manner that you will not be identified.

A.1.8 Confidentiality. The data captured for the research does not include any personally identifiable information about you other than your Prolific ID. Your IP address will not be captured. Do NOT disclose any private or personally identifiable information about yourself or anyone else during this survey.

A.1.9 Right to Ask Questions & Contact Information. If you have any questions about this study, you should feel free to ask them by contacting the Principal Investigator now at iot-labels-study@lists.andrew.cmu.edu. If you have questions later, desire additional information, or wish to withdraw your participation, please contact the Principal Investigator by e-mail in accordance with the contact information listed above. If you have questions pertaining to your rights as a research participant; or to report concerns to this study, you should contact the Office of Research integrity and Compliance at Carnegie Mellon University. Email: irb-review@andrew.cmu.edu. Phone: 412-268-4721.

A.1.10 Voluntary Participation. Your participation in this research is voluntary. You may discontinue participation at any time during the research activity. You may print a copy of this consent form for your records.

Screening question 1. I have read and understand the information above.

- Yes

- No

Screening question 2. I am age 18 or older.

- Yes
- No

Screening question 3. I want to participate in this research and continue with the survey.

- Yes
- No

Instructions: Please do your best to answer each question. When filling out this survey, do NOT disclose any private or personally identifiable information about yourself or anyone else. If you run into any issues with the survey, please do not hesitate to contact us.

A.2 Pre-screen survey

Q1 What is your Prolific ID? (Note: You must enter your real, valid Prolific ID to receive payment for this study) (*free response field*)

Q2 Which gender best describes you?

- Male
- Female
- Non-Binary
- Prefer to self-describe

Q3 Age Which age group do you fall under?

- 18-35
- 36-53
- 54 or above

Q4 Do you have a degree or have you been employed in Engineering or Computer Science or similar technical fields?

- Yes
- No

Q5 How many IoT devices have you purchased online over the last 3 years? (*free response field*)

Q6 How many IoT devices have you purchased in-store over the last 3 years? (*free response field*)

Q7 If you qualify, would you like to participate in a 20-minute survey about IoT devices for \$5 compensation? (Note: You would be taking this survey immediately after the completion of this survey, and it should be completed in one sitting.)

- Yes
- No

Q8 Please provide the names of the IoT devices that you have purchased within the last 3 years in the box below. If you have not purchased any IoT devices in the last 3 years, please write "None." (*free response field*)

A.3 Main Survey

Answer choices are shown in bullets below each question. Answer responses with the text "Other" included a free response box for participants to explain their answers. Participants are presented with three labels at the beginning of the survey, which they will use throughout the survey to answer the questions. The same set of questions is presented to participants assigned to different complexity groups but with different labels.

Imagine you are shopping in a store and you see three smart thermostats on the shelf that have the features you are looking for and are all about the same price. Each package has a label on it with the U.S. Cyber Trust Mark. [participants are shown three labels, one for Sustios, one for EcoHouse, and one for All4Home]

Q1 If you saw these three labels on their product packaging, would you consider them as you shop? Which of the following actions would you take? Participants could select multiple options

- I would not use them at all
- I would glance at them
- I would thoroughly examine the labels
- I would look for anything that looks particularly bad/concerning
- I would scan the QR codes
- I would carefully compare the labels
- I would look for anything that looks particularly good

Q2 Assuming that all three devices have identical functionality, very similar price, and you have decided that you want to buy this kind of thermostat, which of the three devices are you most likely to purchase given the information on the labels?

- All4Home
- EcoHouse
- Sustios
- I would not purchase any of the three devices
- I do not have sufficient information to make this decision

Q3(a) (For participants who chose Sustios for Q2) You chose the Sustios Voice-Activated Thermostat. To what extent do you agree with the following reasons for choosing Sustios over All4Home?

- (1) Sustios has better privacy than All4home
 - I do not see this information on the label
 - Strongly disagree(1)
 - 2
 - Neutral(3)
 - 4
 - Strongly agree(5)
- (2) Sustios has better security than All4Home
 - I do not see this information on the label
 - Strongly disagree(1)
 - 2
 - Neutral(3)
 - 4
 - Strongly agree(5)
- (3) Sustios has better functionality than All4Home
 - I do not see this information on the label
 - Strongly disagree(1)
 - 2
 - Neutral(3)
 - 4
 - Strongly agree(5)

Q3(b) (For participants who chose Sustios for Q2) You chose the Sustios Voice-Activated Thermostat. To what extent do you agree with the following reasons for choosing Sustios over EcoHouse?

- (1) Sustios has better privacy than EcoHouse
 - I do not see this information on the label
 - Strongly disagree(1)
 - 2
 - Neutral(3)
 - 4
 - Strongly agree(5)
- (2) Sustios has better security than EcoHouse
 - I do not see this information on the label
 - Strongly disagree(1)
 - 2
 - Neutral(3)
 - 4
 - Strongly agree(5)
- (3) Sustios has better functionality than EcoHouse
 - I do not see this information on the label
 - Strongly disagree(1)
 - 2

- Neutral(3)
- 4
- Strongly agree(5)

Q3(a) (For participants who chose EcoHouse for Q2) You chose the EcoHouse Voice-Activated Thermostat. To what extent do you agree with the following reasons for choosing EcoHouse over All4Home?

- (1) EcoHouse has better privacy than All4Home
 - I do not see this information on the label
 - Strongly disagree(1)
 - 2
 - Neutral(3)
 - 4
 - Strongly agree(5)
- (2) EcoHouse has better security than All4Home
 - I do not see this information on the label
 - Strongly disagree(1)
 - 2
 - Neutral(3)
 - 4
 - Strongly agree(5)
- (3) EcoHouse has better functionality than All4Home
 - I do not see this information on the label
 - Strongly disagree(1)
 - 2
 - Neutral(3)
 - 4
 - Strongly agree(5)

Q3(b) (For participants who chose EcoHouse for Q2) You chose the EcoHouse Voice-Activated Thermostat. To what extent do you agree with the following reasons for choosing EcoHouse over Sustios?

- (1) EcoHouse has better privacy than Sustios
 - I do not see this information on the label
 - Strongly disagree(1)
 - 2
 - Neutral(3)
 - 4
 - Strongly agree(5)
- (2) EcoHouse has better security than Sustios
 - I do not see this information on the label
 - Strongly disagree(1)
 - 2
 - Neutral(3)
 - 4
 - Strongly agree(5)
- (3) EcoHouse has better functionality than Sustios
 - I do not see this information on the label
 - Strongly disagree(1)
 - 2
 - Neutral(3)
 - 4
 - Strongly agree(5)

Q3(a) (For participants who chose All4Home for Q2) You chose the All4Home Voice-Activated Thermostat. To what extent do you agree with the following reasons for choosing All4Home over EcoHouse?

- (1) All4Home has better privacy than EcoHouse
 - I do not see this information on the label
 - Strongly disagree(1)
 - 2
 - Neutral(3)
 - 4
 - Strongly agree(5)

- (2) All4Home has better security than EcoHouse
 - I do not see this information on the label
 - Strongly disagree(1)
 - 2
 - Neutral(3)
 - 4
 - Strongly agree(5)
- (3) All4Home has better functionality than EcoHouse
 - I do not see this information on the label
 - Strongly disagree(1)
 - 2
 - Neutral(3)
 - 4
 - Strongly agree(5)

Q3(b)(For participants who chose All4Home for Q2) You chose the All4Home Voice-Activated Thermostat. To what extent do you agree with the following reasons for choosing All4Home over Sustios?

- (1) All4Home has better privacy than Sustios
 - I do not see this information on the label
 - Strongly disagree(1)
 - 2
 - Neutral(3)
 - 4
 - Strongly agree(5)
- (2) All4Home has better security than Sustios
 - I do not see this information on the label
 - Strongly disagree(1)
 - 2
 - Neutral(3)
 - 4
 - Strongly agree(5)
- (3) All4Home has better functionality than Sustios
 - I do not see this information on the label
 - Strongly disagree(1)
 - 2
 - Neutral(3)
 - 4
 - Strongly agree(5)

Q3(c)(For participants who chose "I would not purchase any of the three devices" for Q2) Which of the following best describes the reason(s) why you do not want to purchase any of the devices?

- None of these devices meet my security expectations
- None of these devices meet my privacy expectations
- None of these devices meet my functionality expectations
- Other (free response field)

Q3(d)(For participants who chose "I do not have sufficient information to make this decision" for Q2) How helpful would additional information about each of the following factors be to you when making a purchasing decision?

- (1) Data selling practices
 - Not at all helpful(1)
 - 2
 - Neutral(3)
 - 4
 - Very helpful(5)
- (2) Data sharing practices
 - Not at all helpful(1)
 - 2
 - Neutral(3)
 - 4
 - Very helpful(5)
- (3) Data retention practices

- Not at all helpful(1)
- 2
- Neutral(3)
- 4
- Very helpful(5)
- (4) Data storage practices
 - Not at all helpful(1)
 - 2
 - Neutral(3)
 - 4
 - Very helpful(5)
- (5) Access control
 - Not at all helpful(1)
 - 2
 - Neutral(3)
 - 4
 - Very helpful(5)
- (6) Security updates
 - Not at all helpful(1)
 - 2
 - Neutral(3)
 - 4
 - Very helpful(5)
- (7) Sensor Used
 - Not at all helpful(1)
 - 2
 - Neutral(3)
 - 4
 - Very helpful(5)

Q4 Which of the following do you think best describes what the presence of the Cyber Trust Mark on the label represents? [Correct answer: This IoT device passes minimum security and privacy requirements]

- This IoT device has been tested and certified by the government
- This IoT device has been tested and certified by an independent organization
- This IoT device has very good security features
- This IoT device has very good privacy practices
- This IoT device has best-in-class security and privacy practices
- This IoT device passes minimum security and privacy requirements
- I'm not sure

Q5 Which device uses a camera or other visual sensor? [Correct answer: EcoHouse]

- All4Home
- EcoHouse
- Sustios
- None of the devices uses a visual sensor
- There isn't enough information on the labels to determine this
- I don't understand the information on the label

Q6 Which device shares data with ONLY the manufacturer and service providers? [Correct answer: All4Home]

- All4Home
- EcoHouse
- Sustios
- None of the devices share data with only the manufacturer and service providers
- There isn't enough information on the labels to determine this
- I don't understand the information on the label

Q7 Which device sells data to third parties? [Correct answer: EcoHouse]

- All4Home
- EcoHouse
- Sustios

- None of the devices sell data to third parties
- There isn't enough information on the labels to determine this
- I don't understand the information on the label

Q8 Which device provides consent-based security updates? [Correct answer: Sustios]

- All4Home
- EcoHouse
- Sustios
- None of the devices provide automatic security updates
- There isn't enough information on the labels to determine this
- I don't understand the information on the label

Q9 Did you attempt to scan the QR code on any of the labels? If so, how many labels did you scan?

- Did not scan any of the labels
- 1 label scanned
- 2 labels scanned
- 3 labels scanned

Q10 If you saw a label like this when actually shopping for an IoT device, how likely would you be to scan the QR code for more information?

- Very unlikely(1)
- 2
- Neutral(3)
- 4
- Very likely(5)

Q11 If you were looking at a box containing an IoT device in a store and saw a label with a QR code, what would you be most likely to do if you wanted to see more information?

- Scan the QR code with my phone
- Search online for more product information using the search engine of your choice
- Visit the manufacturer's website to look for information
- I wouldn't look for more information
- I'm not sure
- Other (free response field)

Q12 (For participants claimed to have NOT scanned the QR code according to Q9) Which of the following best describes why you wouldn't be likely to scan the QR code?

- I don't know how to scan QR codes
- My phone can't scan QR codes
- It is difficult to scan QR codes with my phone
- I'm worried that scanning QR codes could be insecure
- I wouldn't want to take the time to scan the QR codes
- I'm not that interested in the information I think I would see if I scanned the QR code
- Other (free response field)

Q13 (For participants claimed to have NOT scanned the QR code according to Q9) Which of the following best describes what you would expect to find after scanning the QR code?

- User manual for the device
- Manufacturer's website
- More information about the device's privacy and security
- More product information
- I don't know

Q14 (For participants claimed to have scanned the QR code according to Q9) How easy was it for you to scan the QR code(s)?

- Very easy(1)
- 2
- Neither easy nor difficult(3)
- 4

- Very difficult(5)

Q15 (For participants claimed to have scanned the QR code according to Q9) How easy was it for you to use the label(s) accessed by scanning the QR code to make your purchase decision?

- Very easy(1)
- 2
- Neither easy nor difficult(3)
- 4
- Very difficult(5)

Q16 (For participants who answered 4/5 for Q14) Why did you say it was difficult to scan the QR code? (participants could select multiple options)

- It took a long time for the information to load
- My phone had trouble recognizing the QR code
- The QR code scanner on my phone doesn't always work properly
- Other (free response field)

Q17 (For participants who answered 4/5 for Q15) Why did you find the labels accessed through the QR codes difficult to use? (participants could select multiple options)

- They were too small to read on my phone
- I didn't understand the information in the labels
- The labels didn't contain useful information
- I could only see one label at a time on my phone
- Other (free response field)

Q18 (participants are only shown the attributes that are on their respective packaging labels) How well do you feel you understand what each of the following label elements conveys?

- (1) QR Code
 - Completely do not understand(1)
 - 2
 - Neutral(3)
 - 4
 - Completely understand(5)
- (2) Cyber Trust Mark
 - Completely do not understand(1)
 - 2
 - Neutral(3)
 - 4
 - Completely understand(5)
- (3) Data collection
 - Completely do not understand(1)
 - 2
 - Neutral(3)
 - 4
 - Completely understand(5)
- (4) Data shared
 - Completely do not understand(1)
 - 2
 - Neutral(3)
 - 4
 - Completely understand(5)
- (5) Security updates
 - Completely do not understand(1)
 - 2
 - Neutral(3)
 - 4
 - Completely understand(5)
- (6) Access control
 - Completely do not understand(1)
 - 2
 - Neutral(3)
 - 4

- Completely understand(5)
- (7) Sensor data
 - Completely do not understand(1)
 - 2
 - Neutral(3)
 - 4
 - Completely understand(5)

Q20 (participants are only shown the attributes that are on their respective packaging labels) How much does each of the following label elements influence your decision about which product to purchase?

- (1) QR Code
 - Not influential at all(1)
 - 2
 - Neutral(3)
 - 4
 - Extremely influential(5)
- (2) Cyber Trust Mark
 - Not influential at all(1)
 - 2
 - Neutral(3)
 - 4
 - Extremely influential(5)
- (3) Data collection
 - Not influential at all(1)
 - 2
 - Neutral(3)
 - 4
 - Extremely influential(5)
- (4) Data shared
 - Not influential at all(1)
 - 2
 - Neutral(3)
 - 4
 - Extremely influential(5)
- (5) Security updates
 - Not influential at all(1)
 - 2
 - Neutral(3)
 - 4
 - Extremely influential(5)
- (6) Access control
 - Not influential at all(1)
 - 2
 - Neutral(3)
 - 4
 - Extremely influential(5)
- (7) Sensor data
 - Not influential at all(1)
 - 2
 - Neutral(3)
 - 4
 - Extremely influential(5)
- (8) Information displayed after scanning the QR code
 - Not influential at all(1)
 - 2
 - Neutral(3)
 - 4
 - Extremely influential(5)

Q22 Overall, how helpful did you find the information on the packaging label (before scanning the QR code) in making your purchasing decision?

- Not helpful at all(1)

- 2
- Neutral(3)
- 4
- Extremely helpful(5)

Q23 (For participants claimed to have scanned the QR code according to Q9) Overall, how helpful did you find the information accessed by scanning the QR code in making a purchasing decision?

- Not helpful at all(1)
- 2
- Neutral(3)
- 4
- Extremely helpful(5)

Q24 What do you think about the amount of information on the labels (before scanning the QR code) shown above?

- Too much information
- About the right amount of information
- Not enough information
- I don't know

Q25 (For participants claimed to have scanned the QR code according to Q9) What do you think about the amount of information on the labels you saw by scanning the QR codes?

- Too much information
- About the right amount of information
- Not enough information
- I don't know

Q26 (For participants claimed to have scanned the QR code according to Q9) How convenient did you find retrieving information using the QR code?

- Not convenient(1)
- 2
- Neutral(3)
- (4)
- Extremely convenient(5)

Q27 (For participants claimed to have scanned the QR code according to Q9) What additional information about security or privacy, if any, would be useful for you to see on the label you viewed (shown above) after scanning the QR code? (*free response field*)

Q27 (For participants claimed to have NOT scanned the QR code according to Q9) What additional information about security and privacy, if any, would be useful for you to see on the label on the product packaging? (*free response field*)

Q28 When you are shopping for an IoT device, which of the four label designs above would you be most interested in seeing on the product packaging? (Note: These are all labels for the same device.) [*participants are shown here four labels for Sustios of various complexities*]

- Label 1
- Label 2
- Label 3
- Label 4

Q29 Why did you choose the option you selected for the previous question? (*free response field*)

Q30 When you are shopping for an IoT device, which of these label designs (if any) would you like to see after you scan the QR Code on the label on product packaging? (Note: you must select a different label design from what you selected above.)

- Label 1
- Label 2
- Label 3
- Label 4

Q31 When you are purchasing an IoT device, how important are the following to you?

- (1) Strong privacy
 - Not important at all(1)
 - 2
 - Moderately important(3)
 - 4
 - Absolutely essential(5)
- (2) Strong security
 - Not important at all(1)
 - 2
 - Moderately important(3)
 - 4
 - Absolutely essential(5)
- (3) Device functionality
 - Not important at all(1)
 - 2
 - Moderately important(3)
 - 4
 - Absolutely essential(5)
- (4) Brand reputation
 - Not important at all(1)
 - 2
 - Moderately important(3)
 - 4
 - Absolutely essential(5)
- (5) Ease of use
 - Not important at all(1)
 - 2
 - Moderately important(3)
 - 4
 - Absolutely essential(5)
- (6) Price
 - Not important at all(1)
 - 2
 - Moderately important(3)
 - 4
 - Absolutely essential(5)

Q32 How well do you agree with each of the following statements?

- (1) I typically read privacy policies
 - Strongly disagree(1)
 - 2
 - Neutral(3)
 - 4
 - Strongly agree(5)
- (2) I am extremely motivated to take all the steps needed to keep my online data and accounts safe
 - Strongly disagree(1)
 - 2
 - Neutral(3)
 - 4
 - Strongly agree(5)
- (3) I have adjusted my browser settings to block some or all cookies or have installed a browser extension to do so
 - Strongly disagree(1)
 - 2
 - Neutral(3)
 - 4
 - Strongly agree(5)
- (4) I typically enable two-factor authentication when it is available
 - Strongly disagree(1)
 - 2
 - Neutral(3)
 - 4

- Strongly agree(5)

Q33 Suppose the label you were shown throughout the survey (pictured above) is used for other IoT devices in the market. How would you improve the label itself (e.g. its design, layout, types of information presented)? (*free response field*)

B EDUCATIONAL INTERVENTIONS

Answer choices are shown in bullets below each question.

The new US cybersecurity certification and labeling program is designed to help Americans more easily choose smart devices that are safer and less vulnerable to cyberattacks. Products that include the “U.S. Cyber Trust Mark”, pictured below, on their packaging or website meet baseline standards for cyber security and privacy. You can scan the accompanying QR code to get more information about the product’s security and privacy attributes. [*participants are shown an image of the U.S. Cyber Trust Mark here.*]

Q1 Which of the following do you think best describes what the presence of the Cyber Trust Mark on the label represents?

- This IoT device has been tested and certified by an independent organization
- This IoT device passes minimum security and privacy requirements
- This IoT device has been tested and certified by the government
- This IoT device has very good privacy practices
- This IoT device has very good security features
- This IoT device has best-in-class security and privacy practices

Q2 Which of the following best describes what you would expect to find after scanning the QR code?

- User manual for the device
- Manufacturer’s website
- More information about the device’s privacy and security
- More product information

C LIST OF QUALIFYING DEVICES

- Smart TV (e.g. Samsung, LG, JVC)
- Activity tracker excluding smart watches (e.g. Fitbit, Xiaomi Mi Band, Microsoft band)
- Smart Thermostat (e.g. Nest, Hive, tado)
- Connected lights (e.g. Phillips Hue, LIFX, Elgato Avea, Belkin WeMo)
- Home assistants/smart hub (e.g. Amazon echo, CastleHub, Google Home)
- Smart watch (e.g. Apple watch, Samsung gear, Moto 360, Asus Zen-Watch)
- Video streaming product (e.g. AppleTV, chromecast), Connected printers (e.g. WiFi)
- Smart plugs (e.g. Belkin WeMo Insight Switch)
- Ankuoo NEO PRO Wi-Fi Smart Switch)
- Smart doorlock and/or doorbell (e.g. August Smartlock, Danalock, Ring smart doorbell)
- Smart security camera (e.g. Nest Cam, Netatmo, Netgear Arlo)
- Baby camera/monitor (e.g. Withings Smart Baby Monitor, Motorola Baby Monitor Camera)
- Smart water sprinkler/irrigation controllers (e.g. Aifro WaterEco, BlueSpray, Rachio Smart Sprinkler Controller)
- Smart health monitors excluding smart watches (e.g. scales, blood pressure monitors)
- Smart smoke monitors and alarms (e.g. Kepler, Birdi)
- Smart kitchen appliances (e.g. Fridge, oven, kettle, scales, vacuum)
- Smart Bluetooth trackers excluding smart watches (e.g. keyrings to identify lost keys such as Tile, Chipolo, Lapa 2)
- Grocery ordering (e.g. Amazon dash buttons, Hiku, GeniCan)
- Games console (e.g. PS4, Xbox one)

D KUPPER-HAFNER AGREEMENT FOR QUALITATIVE CODING

Table 2: The table contains the Kupper-Hafner agreement rate for qualitative coding.


	Low-complexity		Medium-complexity		High-complexity	
	Scanned	Did not scan	Scanned	Did not scan	Scanned	Did not scan
q27 - What additional information about security or privacy, if any, would be useful for you to see on the label (you viewed after scanning/on the product packaging)?	0.690	0.704	0.760	0.688	0.585	0.668
q33 - Suppose the label you were shown throughout the survey is used for other IoT devices in the market. How would you improve the label itself?	0.590		0.757		0.653	
q29 - Why did you choose the option you selected for the previous question?	0.669					

E HIGH-COMPLEXITY LABEL ACCESSED VIA QR CODE


Security & Privacy Facts


Sustios





Smart Voice-activated Thermostat 4M0G
Firmware version: 1.3 - updated on: 07/31/2023
The device was manufactured in: China




U.S. CYBER TRUST MARK

 Security Mechanisms	Security updates	Consent-based - Available until at least 08/30/2026			
	Access control	Password - User Generated, Multi-Factor Authentication			



Data Practices

Sensor data collection	 Audio	 Visual	 Physiological	 Location
Sensor type	Microphone			
Purpose	Providing and improving device functions			
Data stored on device	Aggregated or anonymized			
Data stored on cloud	Aggregated or anonymized			
Shared with	Manufacturer			
Sold to	None			
Other collected data	Motion, Account info, Contact info, Device setup info, Device usage info, Temperature, Humidity			

Privacy policy iotregistry.us/sustios/4M0G/privacy


More Information

Detailed Security & Privacy Label:
[Click for More Detailed Information](#)




CMU IoT Security and Privacy Label CISPL 1.0 iotsecurityprivacy.org PUBLIC DOMAIN

Figure 24: The high-complexity label for Sustios with a button that, when clicked, redirects to the ultra-high-complexity label

F COMPLETE STATISTICAL RESULTS

Table 3: This table contains the complete statistical results for survey questions based on label complexity.

Question Text	Label Complexity (Overall)	Label Complexity (Low vs. Mid)	Label Complexity (Low vs. High)	Label Complexity (Mid vs. High)
Q1 - If you saw these three labels on their product packaging, would you consider them as you shop? Which of the following actions would you take?				
A. I would thoroughly examine the labels	< 0.001	< 0.001	0.006	0.469
B. I would carefully compare the labels	< 0.001	< 0.001	< 0.002	0.040
C. I would look for anything that looks particularly bad/concerning.	< 0.001	< 0.001	< 0.001	0.897
D. I would glance at them	0.004	0.017	0.004	0.810
E. I would look for anything that looks particularly good	0.055	0.169	0.019	0.568
F. I would not use them at all	0.865	-	-	-
G. I would look for anything that looks particularly good	<0.001	0.002	0.001	0.915
Q2 - Which of the three devices are you most likely to purchase given the information on the labels?	<0.001	<0.001	<0.001	0.010
Q3(a)(i) - You chose the Sustios Voice-Activated Thermostat. To what extent do you agree with the following reasons for choosing Sustios over All4Home?				
A. Sustios has better privacy than All4Home	0.568	-	-	-
B. Sustios has better security than All4Home	0.019	0.700	0.004	0.019
C. Sustios has better functionality than All4Home	0.091	0.991	0.366	0.038
Q3(b)(i) - You chose the Sustios Voice-Activated Thermostat. To what extent do you agree with the following reasons for choosing Sustios over EcoHouse?				
A. Sustios has better privacy than EcoHouse	0.900	-	-	-
B. Sustios has better security than EcoHouse	0.004	0.220	0.987	0.002
C. Sustios has better functionality than EcoHouse	0.163	-	-	-
Q3(a)(ii) - You chose the All4Home Voice-Activated Thermostat. To what extent do you agree with the following reasons for choosing All4Home over EcoHouse?				
A. All4Home has better privacy than EcoHouse	0.925	-	-	-
B. All4Home has better security than EcoHouse	0.545	-	-	-
C. All4Home has better functionality than EcoHouse	0.163	-	-	-
Q3(b)(ii) - You chose the All4Home Voice-Activated Thermostat. To what extent do you agree with the following reasons for choosing All4Home over Sustios?				
A. All4Home has better privacy than Sustios	0.565	-	-	-
B. All4Home has better security than Sustios	0.761	-	-	-
C. All4Home has better functionality than Sustios	0.166	-	-	-
Q3(a)(iii) - You chose the EcoHouse Voice-Activated Thermostat. To what extent do you agree with the following reasons for choosing EcoHouse over All4Home?				
A. EcoHouse has better privacy than All4Home	0.287	-	-	-
B. EcoHouse has better security than All4Home	0.469	-	-	-
C. EcoHouse has better functionality than All4Home	0.802	-	-	-
Q3(b)(iii) - You chose the EcoHouse Voice-Activated Thermostat. To what extent do you agree with the following reasons for choosing EcoHouse over Sustios?				

Continued on the next page

Table 3 – continued from the previous page

Question Text	Label Complexity (Overall)	Label Complexity (Low vs. Mid)	Label Complexity (Low vs. High)	Label Complexity (Mid vs. High)
A. EcoHouse has better privacy than Sustios	0.925	-	-	-
B. EcoHouse has better security than Sustios	0.991	-	-	-
C. EcoHouse has better functionality than Sustios	0.750	-	-	-
Q3(d) - How helpful would additional information about each of the following factors be to you when making a purchasing decision?				
A. Data selling practices	0.761	-	-	-
B. Data sharing practices	0.234	-	-	-
C. Data retention practices	0.987	-	-	-
D. Data storage practices	0.925	-	-	-
E. Access control	0.366	-	-	-
F. Security updates	0.198	-	-	-
G. Sensors used	0.925	-	-	-
Q4 - Which of the following do you think best describes what the presence of the Cyber Trust Mark on the label represents?	0.377	-	-	-
Q5 - Which device uses a camera or other visual sensor?	0.002	0.002	0.002	1.000
Q6 - Which device shares data with ONLY the manufacturer and service providers?	0.002	0.002	0.002	0.002
Q7 - Which device sells data to third parties?	0.002	0.002	0.002	0.002
Q8 - Which device provides consent-based security updates?	0.002	0.002	0.002	0.002
Q9 - Did you attempt to scan the QR code on any of the labels? If so, how many labels did you scan?	0.002	0.002	0.002	0.188
Q10 - If you saw a label like this when actually shopping for an IoT device, how likely would you be to scan the QR code for more information?	0.218	-	-	-
Q11 - If you were looking at a box containing an IoT device in a store and saw a label with a QR code, what would you be most likely to do if you wanted to see more information?	0.915	-	-	-
Q12 - Which of the following best describes what you would expect to find after scanning the QR code?	0.319	-	-	-
Q13 - Which of the following best describes what you would expect to find after scanning the QR code?	0.399	-	-	-
Q14 - How easy was it for you to scan the QR code(s)?	0.496	-	-	-
Q15 - How easy was it for you to use the label(s) accessed by scanning the QR code to make your purchase decision?	0.666	-	-	-
Q22 - Overall, how helpful did you find the information on the packaging label (before scanning the QR code) in making your purchasing decision?	< 0.001	< 0.001	< 0.001	< 0.001
Q23 - Overall, how helpful did you find the information accessed by scanning the QR code in making a purchasing decision?	0.295	-	-	-
Q24 - What do you think about the amount of information on the labels (before scanning the QR code) shown above?	0.002	0.002	0.002	0.002
Q25 - What do you think about the amount of information on the labels you saw by scanning the QR codes?	0.631	-	-	-

Continued on the next page

Table 3 – continued from the previous page

Question Text	Label Complexity (Overall)	Label Complexity (Low vs. Mid)	Label Complexity (Low vs. High)	Label Complexity (Mid vs. High)
Q26 - How convenient did you find retrieving information using the QR code?	0.582	-	-	-
Q28 - When you are shopping for an IoT device, which of the four label designs above would you be most interested in seeing on the product packaging? (Note: These are all labels for the same device.)	0.002	0.002	0.332	0.030
Q30 - When you are shopping for an IoT device, which of these label designs (if any) would you like to see after you scan the QR Code on the label on product packaging? (Note: you must select a different label design from what you selected above.)	0.991	-	-	-
Q31 - When you are purchasing an IoT device, how important are the following to you?				
A. Strong privacy	0.925	-	-	-
B. Strong security	0.786	-	-	-
C. Device functionality	0.545	-	-	-
D. Brand reputation	0.817	-	-	-
E. Ease of use	0.917	-	-	-
F. Price	0.666	-	-	-
Q32 - How well do you agree with each of the following statements?				
A. I typically read privacy policies	0.250	-	-	-
B. I am extremely motivated to take all the steps needed to keep my online data and accounts safe	0.255	-	-	-
C. I have adjusted my browser settings to block some or all cookies or have installed a browser extension to do so	0.666	-	-	-
D. I typically enable two-factor authentication when it is available	0.689	-	-	-

Table 4: The table contains statistical results from significance tests of survey responses between participants who received educational intervention versus those who did not.

Question Text	Education vs. No Education
Table 4 – Continued from previous page	
Question Text	Education
Q4 - Which of the following do you think best describes what the presence of the Cyber Trust Mark on the label represents?	0.003
Q13 - Which of the following best describes what you would expect to find after scanning the QR code?	0.003
Q18 - How well do you feel you understand what each of the following label elements conveys?	
A. QR code	0.358
B. Cyber Trust Mark	<0.001
C. Data collected	0.921
D. Data shared	0.689
E. Security updates	0.806
F. Access control	0.600
G. Sensor data	0.535
H. Data Stored	0.900
I. Data Sold	0.667
Q20 - How much does each of the following label elements influence your decision about which product to purchase?	
A. QR code	0.553
B. Cyber Trust Mark	0.003
C. Data collected	0.461
D. Data shared	0.900
E. Security updates	0.701
F. Access control	0.916
G. Sensor data	0.522
H. Data Stored	0.689
I. Data Sold	0.791

Table 5: The table contains the summary of statistical results for scanning behavior (based on web log data).

Participant Groups	p-value
Education vs. No Education (Overall, Number of Labels Scanned)	0.001
Education vs. No Education (Low-complexity group, Number of Labels Scanned)	0.002
Education vs. No Education (Medium-complexity group, Number of Labels Scanned)	0.282
Education vs. No Education (High-complexity group, Number of Labels Scanned)	0.667
Education vs. No Education (Overall, Scanning vs. No Scanning)	0.012

Table 6: The complete statistical results for survey questions based on age, technical background, and gender.

Question Text	Age (Overall)	Age (18-35 vs. 36-53)	Age (18-35 vs. 54+)	Age (36-53 vs. 54+)	Technical Background (Y vs. N)	Gender (Male vs. Non-male)
Q2 - Which of the three devices are you most likely to purchase given the information on the labels?	0.487	-	-	-	0.566	0.925
Q3(a)(i) - You chose the Sustios Voice-Activated Thermostat. To what extent do you agree with the following reasons for choosing Sustios over All4Home?						
A. Sustios has better privacy than All4Home	0.616	-	-	-	0.926	0.926
B. Sustios has better security than All4Home	0.843	-	-	-	0.926	0.569

Continued on next page

Table 6 – Continued from previous page

Question Text	Age (Overall)	Age (18-35 vs. 36-53)	Age (18-35 vs. 54+)	Age (36-53 vs. 54+)	Technical Background (Y vs. N)	Gender (Male vs. Non-male)
C. Sustios has better functionality than All4Home	0.900	-	-	-	0.807	0.727
Q3(b)(i) - You chose the Sustios Voice-Activated Thermostat. To what extent do you agree with the following reasons for choosing Sustios over EcoHouse?						
A. Sustios has better privacy than EcoHouse	0.988	-	-	-	0.462	0.989
B. Sustios has better security than EcoHouse	0.667	-	-	-	0.725	0.926
C. Sustios has better functionality than EcoHouse	0.859	-	-	-	0.767	0.926
Q3(a)(ii) - You chose the All4Home Voice-Activated Thermostat. To what extent do you agree with the following reasons for choosing All4Home over EcoHouse?						
A. All4Home has better privacy than EcoHouse	0.719	-	-	-	0.727	0.991
B. All4Home has better security than EcoHouse	0.900	-	-	-	0.569	0.922
C. All4Home has better functionality than EcoHouse	0.926	-	-	-	0.264	0.922
Q3(b)(ii) - You chose the All4Home Voice-Activated Thermostat. To what extent do you agree with the following reasons for choosing All4Home over Sustios?						
A. All4Home has better privacy than Sustios	0.121	<0.001	<0.001	0.701	0.991	0.220
B. All4Home has better security than Sustios	0.499	-	-	-	0.991	0.515
C. All4Home has better functionality than Sustios	0.806	-	-	-	0.232	0.926
Q3(a)(iii) - You chose the EcoHouse Voice-Activated Thermostat. To what extent do you agree with the following reasons for choosing EcoHouse over All4Home?						
A. EcoHouse has better privacy than All4Home	0.150	-	-	-	0.107	0.922
B. EcoHouse has better security than All4Home	0.582	-	-	-	0.545	0.543
C. EcoHouse has better functionality than All4Home	0.569	-	-	-	0.398	0.226
Q3(b)(iii) - You chose the EcoHouse Voice-Activated Thermostat. To what extent do you agree with the following reasons for choosing EcoHouse over Sustios?						
A. EcoHouse has better privacy than Sustios	0.802	-	-	-	0.076	0.235
B. EcoHouse has better security than Sustios	0.701	-	-	-	0.739	0.986
C. EcoHouse has better functionality than Sustios	0.864	-	-	-	0.0855	0.170
Q3(d) - How helpful would additional information about each of the following factors be to you when making a purchasing decision?						
A. Data selling practices	0.926	-	-	-	0.701	0.991
B. Data sharing practices	0.991	-	-	-	0.254	0.569
C. Data retention practices	0.956	-	-	-	0.787	0.751
D. Data storage practices	0.922	-	-	-	0.653	0.900
E. Access control	0.926	-	-	-	0.054	0.438
F. Security updates	0.667	-	-	-	0.060	0.145
G. Sensors used	0.783	-	-	-	0.030	0.904
Q4 - Which of the following do you think best describes what the presence of the Cyber Trust Mark on the label represents?	0.034	0.412	0.0235	0.021	0.0710	0.003
Q5 - Which device uses a camera or other visual sensor?	0.600	-	-	-	0.921	0.797
Q6 - Which device shares data with ONLY the manufacturer and service providers?	0.689	-	-	-	0.515	0.806
Q7 - Which device sells data to third parties?	0.610	-	-	-	0.900	0.434

Continued on next page

Table 6 – Continued from previous page

Question Text	Age (Overall)	Age (18-35 vs. 36-53)	Age (18-35 vs. 54+)	Age (36-53 vs. 54+)	Technical Background (Y vs. N)	Gender (Male vs. Non-male)
Q8 - Which device provides consent-based security updates?	0.988	-	-	-	0.070	0.595
Q10 - If you saw a label like this when actually shopping for an IoT device, how likely would you be to scan the QR code for more information?	<0.001	<0.001	<0.001	0.526	0.884	0.269
Q11 - If you were looking at a box containing an IoT device in a store and saw a label with a QR code, what would you be most likely to do if you wanted to see more information?	0.020	0.049	0.020	0.367	0.582	0.717
Q12 - Which of the following best describes what you would expect to find after scanning the QR code?	0.043	0.926	0.020	0.118	0.367	0.667
Q13 - Which of the following best describes what you would expect to find after scanning the QR code?	0.591	-	-	-	0.946	0.725
Q14 - How easy was it for you to scan the QR code(s)?	0.499	-	-	-	0.921	0.925
Q15 - How easy was it for you to use the label(s) accessed by scanning the QR code to make your purchase decision?	0.767	-	-	-	0.806	0.204
Q22 - Overall, how helpful did you find the information on the packaging label (before scanning the QR code) in making your purchasing decision?	0.034	0.011	0.249	0.314	0.945	0.849
Q23 - Overall, how helpful did you find the information accessed by scanning the QR code in making a purchasing decision?	0.665	-	-	-	0.806	0.987
Q24 - What do you think about the amount of information on the labels (before scanning the QR code) shown above?	0.689	-	-	-	0.900	0.921
Q25 - What do you think about the amount of information on the labels you saw by scanning the QR codes?	0.667	-	-	-	0.242	0.667
Q26 - How convenient did you find retrieving information using the QR code?	0.124	0.578	0.0502	0.198	0.807	0.545
Q28 - When you are shopping for an IoT device, which of the four label designs above would you be most interested in seeing on the product packaging? (Note: These are all labels for the same device.)	<0.001	0.105	0.003	0.219	0.194	0.930
Q30 - When you are shopping for an IoT device, which of these label designs (if any) would you like to see after you scan the QR Code on the label on product packaging? (Note: you must select a different label design from what you selected above.)	0.496	-	-	-	0.725	0.922
Q31 - When you are purchasing an IoT device, how important are the following to you?						
A. Strong privacy	0.105	0.203	0.0455	0.667	0.880	0.203
B. Strong security	0.121	0.265	0.048	0.578	0.954	0.925
C. Device functionality	0.219	-	-	-	0.667	0.548
D. Brand reputation	0.216	-	-	-	0.751	0.667
E. Ease of use	0.026	0.843	0.0115	0.049	0.068	0.154
F. Price	0.249	-	-	-	0.198	0.767
Q32 - How well do you agree with each of the following statements?						
A. I typically read privacy policies	<0.001	<0.001	0.032	0.096	0.235	0.595

Continued on next page

Table 6 – Continued from previous page

Question Text	Age (Overall)	Age (18-35 vs. 36-53)	Age (18-35 vs. 54+)	Age (36-53 vs. 54+)	Technical Background (Y vs. N)	Gender (Male vs. Non-male)
B. I am extremely motivated to take all the steps needed to keep my online data and accounts safe	<0.001	<0.001	0.034	0.220	0.012	0.701
C. I have adjusted my browser settings to block some or all cookies or have installed a browser extension to do so	0.085	0.261	0.500	0.030	0.050	0.011
D. I typically enable two-factor authentication when it is available	0.667	-	-	-	0.921	0.070