Ask the Consumers: What Should be on IoT Privacy & Security Labels?

Claire Chen Hamsini Ravishankar Dillon Shu Laxita Jain
Yifeng Zeng Yuvraj Agarwal Lorrie Faith Cranor
Carnegie Mellon University

1 Introduction

Consumers lack an efficient means to access reliable information about security and privacy of Internet of Things (IoT) devices when making purchase decisions. However, consumers still want privacy and security information while making a purchase and report it as a factor influencing their purchase decisions [4]. Building on Kelly et al.'s label for website privacy policies, Emami-Naeini et al. developed a label specifically for IoT devices that provides a quick overview of privacy and security features [2], [6].

We present the results of a preliminary IRB-approved online crowdsourced survey administered to 60 US adults to determine the essential information needed to inform consumers about privacy and security risks on device packaging to facilitate informed purchase and comparison decisions. To assess the effectiveness of information presented on different labels, we adapted our evaluation framework from Habib et al.'s privacy choice evaluation metrics, including user needs, user comprehension, user sentiment, impact on decision making, and ease of use [5].

2 Related Work

Emami-Naeini et al. found that consumers lack awareness of IoT device privacy and security practices, posing potential risks [4]. Furthermore, they found that the following privacy and security attributes most impacted consumers' willingness to purchase IoT devices: the sale and sharing of data to third parties, cloud retention, and access control [3]. They then designed the primary layer of IoT privacy and security labels to encapsulate these attributes. Their two-layer label design also includes a secondary layer that conveys additional information of interest, primarily for experts [1].

Although expert opinion provided the basis for privacy label designs created by Emami-Naeini et al. [1], insights gained from experts may differ from consumer opinion. They called for future work to explore whether information on their design is useful for consumers [2]. In subsequent consumer research, they found that information on the primary layer of their labels helped consumers distinguish devices with more and less risky security and privacy characteristics [3].

3 Methods

We tested three label variants designed for product packaging, as shown in Figure 1. We simplified Agarwal et al.'s compact label mockup for packaging[1] by removing all icons except for the QR code and the shield, resulting in what we refer to as the *low-complexity* label. For the *high-complexity* label, we use Emami-Naeini et al.'s IoT privacy and security label primary layer [1]. The *medium-complexity* label features an attribute list of security and privacy settings—a subset of information found on the high-complexity label.

We recruited 60 US-based participants via Prolific who were at least 18 years old and had reported that they owned an IoT device to take a survey. We used a 15-minute Qualtrics survey to collect consumers' self-reported data and compensated participants $3.00 for successful completion. To minimize the learning effect, we employed a between-subjects design and randomly assigned all participants to three groups of approximately the same size, where each group saw one of low-, medium-, or high-complexity label designs.

The survey featured two scenarios. In the first scenario we asked participants to consider the label on a single device corresponding to their condition, assessing each label design's influence on a consumer's IoT device purchasing decision and acceptance of the device's security and privacy settings. The

[1] See compact label on slide 27 at https://www.iotsecurityprivacy.org/downloads/CarnegieMellon-IoT-labels-WhiteHouse-Oct2022-YuvrajAgarwal.pdf

USENIX Symposium on Usable Privacy and Security (SOUPS) 2023.
August 6–8, 2023, Anaheim, CA, USA

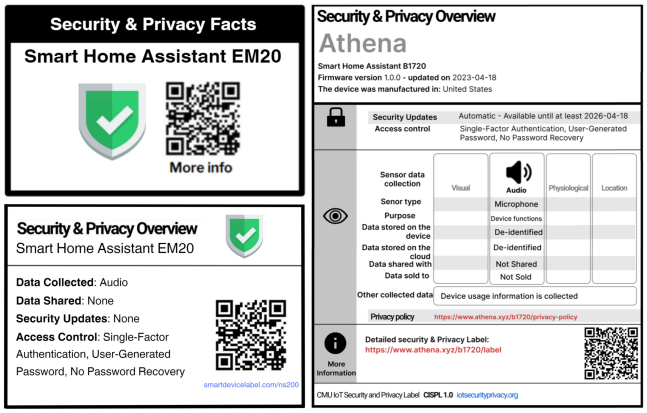

Figure 1: An Example of Low- (top left), Medium- (bottom left), and High- (right) Complexity Labels

second scenario involved assessing the labels' effectiveness in facilitating product comparison, where participants saw three devices that shared identical functionality but varied in terms of their security and privacy practices. Based on the label information, participants needed to decide which of the three products offered the best security and privacy and which they preferred.

To mitigate bot submissions and ensure high quality responses, we implemented three data quality measures: Prolific's prescreening tools, a reCaptcha check, and manual attention checks based on the quality of open-ended responses.

To analyze our free responses, we utilized triple coding. After independently coding the responses, three authors discussed the results until agreement had been reached.

To assess the effectiveness of our IoT privacy and security labels, we adapted our evaluation framework from Habib et al.'s privacy choice evaluation metrics, including user needs, user comprehension, user sentiment, impact on decision making, and ease of use [5]. We designed our survey questions with this framework in mind.

4 Results

Using coded qualitative responses, we found that the majority (13 of 22) in the low-complexity group did not find anything on the label helpful. For the medium-complexity label, 8 of 19 participants mentioned finding access control to be the most helpful element. In the high-complexity label group, data shared (9 of 19) and data collected (9 of 19) were mentioned as helpful.

In addition, 19 of 22 participants shown the low-complexity label desired clarification of label elements. Responses included P42's "everything because there is simply no info" and P50's "what does the green check mark mean?" In contrast, fewer participants shown medium- (9) or high- (11) complexity labels requested clarification. As shown in Figure

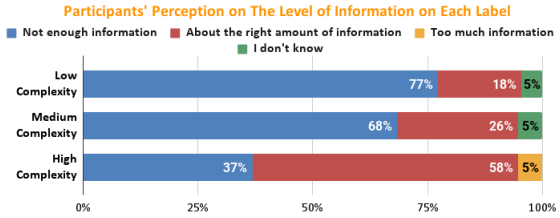

Figure 2: Participant responses to *"What do you think about the amount of information on this label?"*

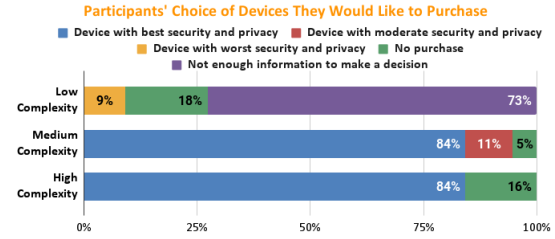

Figure 3: Participant responses to *"Given devices X, Y, and Z, which would you purchase?"* (X = blue, Y = red, Z = yellow)

2, participants in the high-complexity condition were most likely to find the the level of information about right.

In our second scenario, we asked participants to choose the device with the best data protection practices and the device they would like to purchase from three similar devices. 16 of 19 in both medium and high complexity groups correctly chose the most protective device (Figure 3). Similarly, most participant in medium- (16 of 19) and high- (17 of 19) complexity groups also selected the best device, with none incorrectly choosing the worst device. Comparatively, most participants (16 of 22) in the low-complexity group said they were not provided with enough information to make a decision and 20 of 22 in the low-complexity group correctly claimed that they couldn't determine the best device due to insufficient information (Figure 4). Overall, our results suggest that both medium- and high-complexity labels fulfill consumer's basic information needs, but consumers are interested in seeing more information.

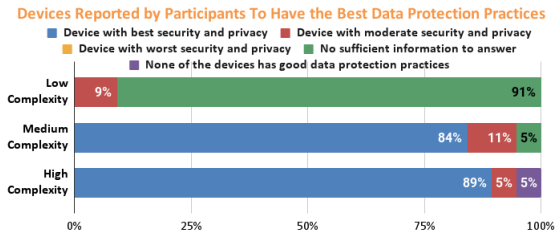

Figure 4: Participant responses to *"Which device do you think has the best data protection practices?"*

References

[1] Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, and Hanan Hibshi. Ask the experts: What should be on an iot privacy and security label? In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 447–464. IEEE, 2020.

[2] Pardis Emami-Naeini, Janarth Dheenadhayalan, Yuvraj Agarwal, and Lorrie Faith Cranor. An informative security and privacy "nutrition" label for internet of things devices. *IEEE Security & Privacy*, 20(2):31–39, 2021.

[3] Pardis Emami-Naeini, Janarth Dheenadhayalan, Yuvraj Agarwal, and Lorrie Faith Cranor. 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)*, pages 519–536. IEEE, 2021.

[4] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. Exploring how privacy and security factor into iot device purchase behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–12, 2019.

[5] Hana Habib and Lorrie Faith Cranor. Evaluating the usability of privacy choice mechanisms. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 273–289, 2022.

[6] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W Reeder. A" nutrition label" for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, pages 1–12, 2009.