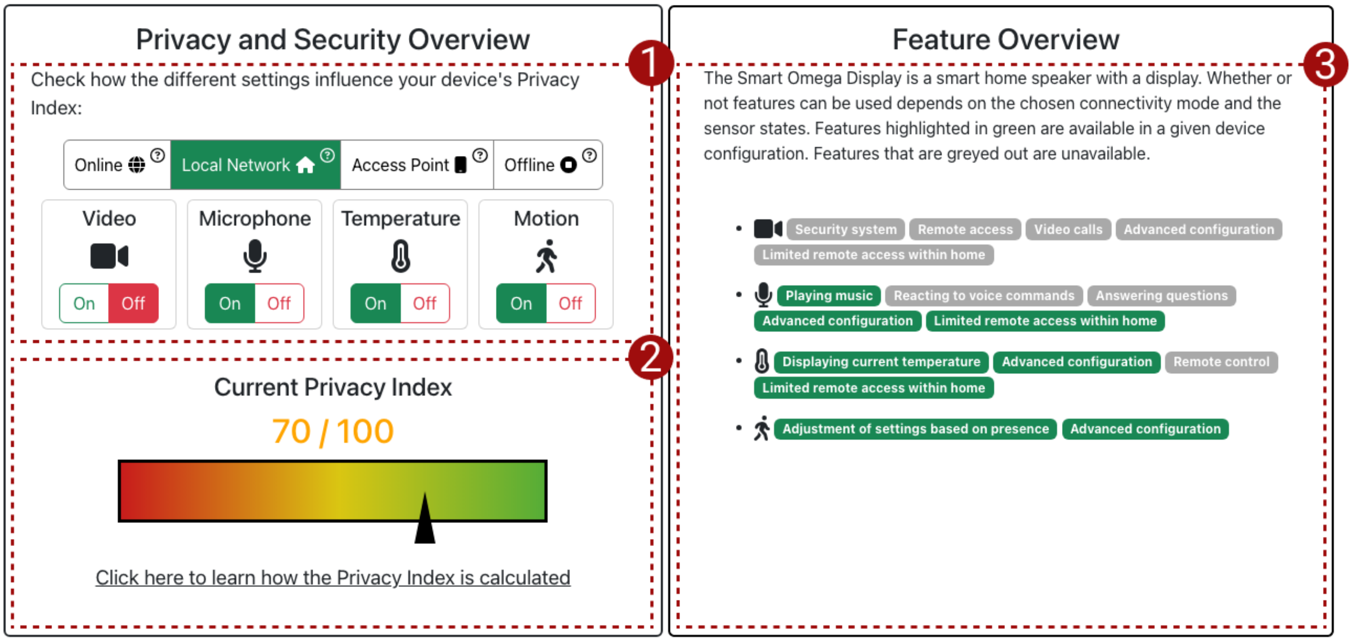
# Designing Interactive Privacy Labels for Advanced Smart Home Device Configuration Options

Maximiliane Windl
LMU Munich
Munich, Germany
Munich Center for Machine Learning
(MCML)
Munich, Germany
maximiliane.windl@ifi.lmu.de

Sebastian S. Feger
LMU Munich
Munich, Germany
TH Rosenheim
Rosenheim, Germany
sebastian.feger@ifi.lmu.de



Check how the different settings influence your device's Privacy Index:

Current Privacy Index

70 / 100

The Smart Omega Display is a smart home speaker with a display. Whether or not features can be used depends on the chosen connectivity mode and the sensor states. Features highlighted in green are available in a given device configuration. Features that are greyed out are unavailable.

**Figure 1: The final *interactive* smart device privacy label, based on an iterative design process with in-depth feedback from expert interviews. The boxes mark the label's key components: (1) the control component that enables users to change the connectivity mode (top) and the state of individual sensors (bottom); (2) the privacy index that reflects the privacy exposure based on the configuration from (1); and (3) a feature overview that dynamically reflects the available feature set based on the configuration (1).**

## ABSTRACT

Labels inform smart home users about the privacy of devices before purchase and during use. Yet, current privacy labels fail to fully reflect the impact of advanced device configuration options like sensor state control. Based on the successful implementation of related privacy and security labels, we designed extended static and interactive labels that reflect sensor states and device connectivity. We first did expert interviews ($N = 10$) that informed the final label design. Second, we ran an online survey ($N = 160$) to assess the interpretation and usability of the novel interactive privacy label. Lastly, we conducted a second survey ($N = 120$) to investigate how well our interactive labels educate users about sensor configuration. We found that most participants successfully used the interactive label and retrieved sensor information more efficiently and correctly. We discuss our findings in the context of a potential shift in label use toward control and use-case-based interaction.

## CCS CONCEPTS

• **Security and privacy** → **Human and societal aspects of security and privacy**; **Social aspects of security and privacy**.

*DIS '24, July 01–05, 2024, IT University of Copenhagen, Denmark*
© 2024 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 979-8-4007-0583-0/24/07
https://doi.org/10.1145/3643834.3661527

## KEYWORDS

Privacy, Smart Home, Privacy Labels, Interactivity

**ACM Reference Format:**

Maximiliane Windl and Sebastian S. Feger. 2024. Designing Interactive Privacy Labels for Advanced Smart Home Device Configuration Options. In *Designing Interactive Systems Conference (DIS '24), July 01–05, 2024, IT University of Copenhagen, Denmark.* ACM, New York, NY, USA, 17 pages. https://doi.org/10.1145/3643834.3661527

## 1 INTRODUCTION

Smart home devices are typically equipped with numerous sensors like microphones and cameras that constantly record and process data from within users' homes. This provides smart home inhabitants with entertainment and automates tedious tasks. Yet, the increasing number and quality of smart device sensors pose privacy risks as the data can be abused to infer sensitive information, reveal identities, or track user behavior [3, 33, 35]. In response, static printed and digital Internet of Things (IoT) privacy and security labels were developed to inform users about their devices before purchase and during device use [13, 14]. These labels were not only very well-received within the academic community but even impacted political programs and standardization initiatives at the highest level: The U.S. announced a cybersecurity labeling program for smart devices[1].

The current labels thoroughly inform users about the device sensors and provide an overview of device security mechanisms. In particular, they provide a sense of sensor recording frequency, data storage, and sharing practices, if applicable, and in case such information is available [13]. However, they do not directly reflect device configuration options and their impact on privacy assessments and device features. This stands in contrast to growing research initiatives around the control and communication of individual device sensor states [10, 12, 41]. Such control options include off-the-shelves mechanisms like buttons that deactivate microphones in smart speakers or physical camera shutters. In particular, tangible sensor control and communication mechanisms have been linked to the inclusiveness of smart device privacy [46]. Following this call for inclusive privacy, we aim to understand how device sensor configuration options can be reflected in privacy labels. Through our research, we extend and adapt current labels [13, 14] by adding information around the user configurability of sensor states, contrasting the privacy risks of different sensor types, and surfacing the impact of sensor state configurations on device features.

We further considered device connectivity modes in line with our goal to reflect increasingly advanced configuration options in privacy labels. Most modern smart devices only function when connected to the internet, raising many privacy concerns and resulting in users temporarily removing them from the network or power outlet [21]. In an effort to provide an alternative to this drastic method, recent work envisioned maintaining smart home device features across four connectivity modes: online, local network, access point, and offline [15]. Our label design incorporated connectivity as a configuration option along these research threads.

As a result, we carefully designed smart home privacy labels that reflect these device configuration options based on the extensive empirical research on IoT privacy and security labels [13, 14]. We created one static, printable label and one digital label that can be accessed through a QR code. In contrast to the current label, our digital label is *interactive* to fully reflect device and sensor configurability. We first evaluated these labels with 10 participants in an expert interview study before refining them based on our findings. Afterward, we conducted an online survey with 160 participants to assess the interpretability and usability of the refined label among a large and diverse user group. Finally, we conducted a second applicability online survey with 120 participants to investigate how well the interactive labels educate users about sensor configuration. Through these studies, our work addresses the following three research questions:

**RQ1** *How can we reflect advanced smart device configuration options in privacy labels?*
**RQ2** *What role does interactivity play in the design of advanced privacy labels?*
**RQ3** *How well does an interactive privacy label educate users about sensor configuration?*

Our findings show that the digital and interactive label is more suitable for mapping advanced device configuration options than the printed static privacy label. We discuss this shift through the lenses of accessibility and usability challenges. Our expert participants further discussed a potential shift in primary label use and new smart home integration options due to the label *interactivity*. Further, we find that the *interactive* label was immediately configured correctly by most participants in our survey study and that many participants selected more privacy-preserving settings than required by the tasks. Finally, our third study showed that participants considered the information provided by the interactive label important and that it helped them find sensor information more efficiently and accurately.

Our work makes the following contributions: (1) We report on the design and implementation of static and interactive smart device privacy labels that map advanced device configuration options around sensor and connectivity control; (2) We present findings from the label evaluation with ten experts and report on the subsequent design adaptation of the interactive label; (3) We report findings from a survey evaluation of the interactive label with 160 participants that surfaced valuable insight regarding feature and privacy trade-off and interactive label usability; (4) we present findings from a second survey with 120 participants that showed that the interactive labels support users in finding sensor information more efficiently and accurately, and (5) we discuss the sum of our findings through the lenses of a potential shift in primary label use due to label *interactivity*, as well as resulting opportunities and challenges related to label accessibility and integration.

## 2 RELATED WORK

In this section, we discuss growing privacy concerns in smart homes and detail the current state of privacy labels before reflecting on the value of incorporating additional smart home privacy control mechanisms.

[1] 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/

## 2.1 Smart Home Privacy Concerns

Privacy in smart homes is subject to exceptional societal and legal expectations, as devices are getting placed in the most intimate spaces, such as bathrooms and bedrooms, putting users in situations where they require absolute privacy [4, 26, 48]. Preserving users’ privacy is especially important as research already showed how the data collected in homes can be exploited to, among others, reveal identities [35], retrace user behavior [3], identify the number of people in a household, or their sleeping routines and eating habits [33]. While users are often unaware of the exact dangers and vulnerabilities posed by smart devices [18, 30, 31], they can formulate concrete concerns when explicitly asked [45]. Such concerns include smart speakers that are always listening [26], targeted advertising, data getting shared with third parties [26], devices transmitting additional data without explicit consent or security loopholes [25]. Using a smart shower head, researchers found that participants did not perceive data as sensitive per se but that it became sensitive through conversations in which the partner became aware of showering habits [24]. Worthy et al. [47] echoed this by stating that data becomes more sensitive when shared with familiar people as they can interpret it more easily. In addition, prior research discussed how smart devices are exploited in abusive partnerships to spy on partners [27]. Hence, whether or not people perceive data misuse as concerning depends on social relationships and situational sensemaking. Regarding different sensor types, users are most concerned about cameras and microphones [9, 34, 45], and mostly do not consider temperature or motion sensors as threatening [44]; some users even doubt that smart devices without cameras or microphones raise any concerns [8, 11, 48].

## 2.2 IoT Privacy Labels

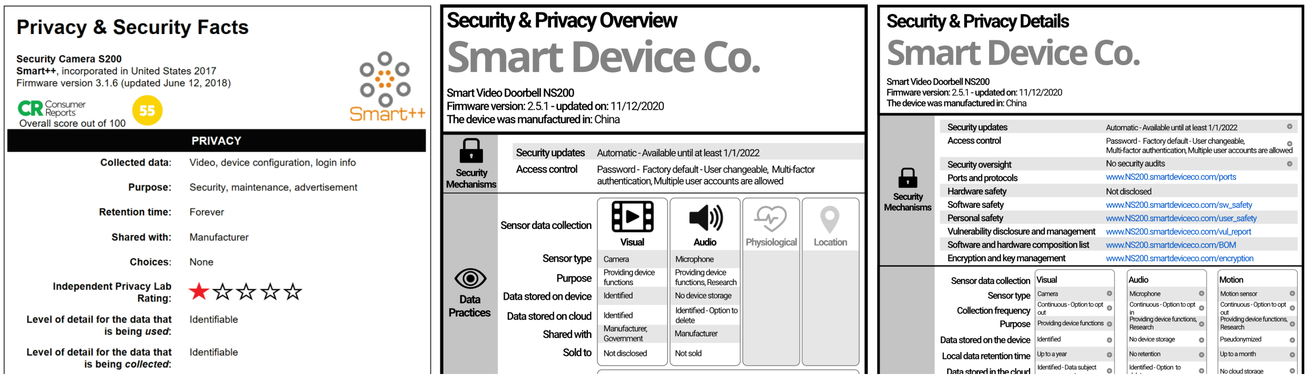
Emami-Naeini et al. [14] interviewed 24 IoT device users about their smart home device purchase behaviors and privacy concerns. The authors were particularly interested in mapping the value that smart device owners assign to privacy and security during device purchase. They further designed a privacy and security prototype label based on common food nutrition labels. This label prototype for one hypothetical device is shown in Figure 2a. As part of their study, the authors asked the participants to review the label for one of three such devices and think aloud. While users perceived the labels as generally helpful in informing their purchase decisions, some participants requested additional information and definitions. In this context, the authors noted that while *“adding all of this information to a static label would likely reduce its usability, additional information can be included in an interactive online label, where consumers can hover over or click on each factor to obtain additional information.”* Such an online label could be retrievable through a QR code included in the static label and printed on the product package. Our work builds upon this notion of label *interactivity*, expanding from additional explanatory information toward actual label configuration.

In their follow-up work, Emami-Naeini et al. [13] first conducted an expert elicitation study that followed a three-round Delphi process to identify those factors and dimensions most important for consumers to compare privacy and security implications of IoT devices. Based on their findings with 22 privacy and security experts, they created primary and secondary privacy and security labels. The primary label is designed to contain the most relevant information and is supposed to be printed on the product package. In contrast, the secondary label contains more detailed and explanatory information. This label is supposed to be retrievable online and linked through a QR code on the primary label. The authors confronted 15 IoT device users with these two label types to understand how consumers use them. To this end, they designed primary and secondary labels for two fictitious brands of security cameras. In their consumer study, all participants noted the current lack of privacy and security information represents an issue during device selection. While most participants appreciated the layered design that allowed them to review devices according to their personal interests, knowledge, and concerns, some noted that accessing the secondary label through a QR code on a mobile phone might represent accessibility challenges for some parts of the population, especially the elderly. Based on the in-depth feedback of the consumers, the authors adapted and finalized the primary and secondary labels, as shown in Figures 2b and 2c. Our work closely builds upon these latest findings and the layered design approach while exploring additional design opportunities related to the *interactivity* of the secondary label.

## 2.3 Advanced Device Configuration Options

Prior research assigned users’ inability to act according to their privacy preferences in the IoT to the lack of clear privacy configuration options [2]. However, some smart device manufacturers recognize users’ diverging privacy preferences and provide built-in mechanisms to shield or deactivate individual sensors – sometimes using simple buttons, sometimes using physical mechanisms such as camera shutters. Such physical mechanisms instill high trust and have been recommended by prior research, as everyone can understand them no matter their technological affinity [1, 9, 46]. With this, physical mechanisms can contribute to inclusive privacy in smart home contexts [46] and Ahmad et al. [1] even call for each sensor in a smart home to have tangible mechanisms to control data collection. Other research efforts to provide tangible sensor level control include a wearable microphone jammer [10], a hat to prevent a smart speaker from listening [41], a smart calendar that only reveals sensitive appointments when placed in a private environment [22], and a smart webcam shutter activated when the camera is not in use [12]. Responding to the call from prior research to enable sensor level control, we address this configuration option in our interactive privacy labels.

One of the most effective measures to prevent smart devices from exposing data is to unplug them from the power supply. In fact, Jin et al. [21] found in their survey study on smart home privacy-protective behaviors with 159 participants that powering off devices is a practice many smart device users employ. Related to devices with a camera, the authors noted 12 reports of users turning off or powering off devices. This increased to 37 reports for smart speakers, and for all other devices, the authors registered four reports. Asked about the most wanted features, the authors documented 27 occurrences of users requesting automated or remote features to turn or power devices off. Notably, the authors found three reports



**Privacy & Security Facts**

**Security Camera S200**
**Smart++**, incorporated in United States 2017
Firmware version 3.1.6 (updated June 12, 2018)

CR Consumer Reports
Overall score out of 100
55
Smart++

**PRIVACY**

| | |
|---|---|
| **Collected data:** | Video, device configuration, login info |
| **Purpose:** | Security, maintenance, advertisement |
| **Retention time:** | Forever |
| **Shared with:** | Manufacturer |
| **Choices:** | None |
| **Independent Privacy Lab Rating:** | ★☆☆☆☆ |
| **Level of detail for the data that is being *used*:** | Identifiable |
| **Level of detail for the data that is being *collected*:** | Identifiable |

(a)

**Security & Privacy Overview**

**Smart Device Co.**

Smart Video Doorbell NS200
**Firmware version:** 2.5.1 - **updated on:** 11/12/2020
**The device was manufactured in:** China

**Security Mechanisms**

| | |
|---|---|
| Security updates | Automatic - Available until at least 1/1/2022 |
| Access control | Password - Factory default - User changeable, Multi-factor authentication, Multiple user accounts are allowed |

**Data Practices**

| Sensor data collection | Visual | Audio | Physiological | Location |
|---|---|---|---|---|
| Sensor type | Camera | Microphone | | |
| Purpose | Providing device functions | Providing device functions, Research | | |
| Data stored on device | Identified | No device storage | | |
| Data stored on cloud | Identified | Identified - Option to delete | | |
| Shared with | Manufacturer, Government | Manufacturer | | |
| Sold to | Not disclosed | Not sold | | |

(b)

**Security & Privacy Details**

**Smart Device Co.**

Smart Video Doorbell NS200
**Firmware version:** 2.5.1 - **updated on:** 11/12/2020
**The device was manufactured in:** China

**Security Mechanisms**

| | |
|---|---|
| Security updates | Automatic - Available until at least 1/1/2022 |
| Access control | Password - Factory default - User changeable, Multi-factor authentication, Multiple user accounts are allowed |
| Security oversight | No security audits |
| Ports and protocols | www.NS200.smartdeviceco.com/ports |
| Hardware safety | Not disclosed |
| Software safety | www.NS200.smartdeviceco.com/sw_safety |
| Personal safety | www.NS200.smartdeviceco.com/user_safety |
| Vulnerability disclosure and management | www.NS200.smartdeviceco.com/vul_report |
| Software and hardware composition list | www.NS200.smartdeviceco.com/BOM |
| Encryption and key management | www.NS200.smartdeviceco.com/encryption |

| Sensor data collection | Visual | Audio | Motion |
|---|---|---|---|
| Sensor type | Camera | Microphone | Motion sensor |
| Collection frequency | Continuous - Option to opt out | Continuous - Option to opt in | Continuous - Option to opt out |
| Purpose | Providing device functions | Providing device functions, Research | Providing device functions, Research |
| Data stored on the device | Identified | No device storage | Pseudonymized |
| Local data retention time | Up to a year | No retention | Up to a month |
| Data stored in the cloud | Identified - Data subject | Identified - Option to | No cloud storage |

(c)

**Figure 2: Overview of the IoT privacy and security labels proposed in related work. For uniform display, the labels have been cut vertically. The complete labels are linked in the following references. (a) First prototype label designed and evaluated by Emami-Naeini et al. [14] in a study with 24 IoT device users. (b) Primary label and (c) secondary label resulting from a follow-up study with 22 experts and 15 IoT consumers [13].**

of participants engaging in network management, and one asked for local-only network communication. In this context, when asked why not to engage in privacy-preserving behaviors, six referred to an "all or nothing dilemma," meaning, for example, one must "sacrifice privacy to use the service."

Along these lines, Feger et al. [15] envisioned future smart device ecosystems that provide features across a wider connectivity spectrum. They also stressed that current smart home appliances are typically rendered useless when disconnected from the internet. In response, they built two smart home devices, a camera and an environmental control unit, that provide features across a connectivity spectrum with four levels: online, local network, access point mode, and offline. Here, access point mode refers to the direct information exchange with one single connected device. A simple label contrasts the trade-off between increased privacy risk exposure due to increased connectivity and a feature decrease that correlates with lower connectivity. Yet, these devices provide valuable features across all connectivity levels. Our work directly connects to these research threads by exploring how advanced connectivity configuration can be reflected in smart device privacy labels.

## 2.4 Quantifying the Impact on Privacy

Jin et al. [21] investigated how smart home users can be supported in privacy-protective behavior. For this, they created 11 storyboards based on a wish list of 159 survey participants. A follow-up evaluation with 227 consumers found that the most favored feature was the envisioned mobile app *Privacy Diagnostics* that offered a concrete privacy score (e.g., 72 / 100) and suggestions on improving the score. The idea of quantifying the impact of privacy with a score is not new and was already suggested in 2010 in connection to social networks [28]. Here, the score should help monitor privacy risks, enable social comparison, and recommend improving the score. Moreover, such a score was also already introduced into privacy labels [5]. Designers created a highly simplified privacy label representing a privacy score with a color scheme and a letter from A to F [16]. Our work builds on this research thread by integrating a quantified value representing a device's privacy impact.

## 2.5 Summary

Smart device privacy and security labels, as designed and evaluated by Emami-Naeini et al. [13, 14], represent strong tools to inform users about the privacy implications of devices and help them make informed purchase decisions. They have been very well-received in the academic and political communities. Yet, there is an opportunity to represent additional information in future smart home device privacy labels, including individual sensor impact, device connectivity, and the impact on privacy. These examples reflect the latest research on sensor state change and communication [46], connectivity control that emphasizes device functionality even if not connected to the internet [15], and quantifying the impact on privacy by implementing a privacy score [21, 28]. Reflecting additional complex information in privacy labels requires exploring new interaction and communication tools. In particular, our work expands on the notion of *interactivity* [14] on the secondary label layer [13]. In this context, we note that initial explorations into *interactive* labels have been reported in the context of nutrition labels [6]. As they miss an empirical evaluation, we expect that findings from our research contribute to consumer label design beyond smart device privacy.

# 3 METHOD

For a visual overview of our method, see Figure 3. First, we created two new label designs based on the key insights from prior work: A static label to be printed on the device box to inform during the purchasing stage and a second interactive label designed to help users explore the impact of different device configurations on privacy. We used these initial label designs for ten expert interviews, where we (1) discussed the designs and (2) explored the potential of interactive labels and the benefits and pitfalls of quantifying a device's impact on privacy. After we used our insights to refine the label designs, we conducted a large-scale online survey with 160

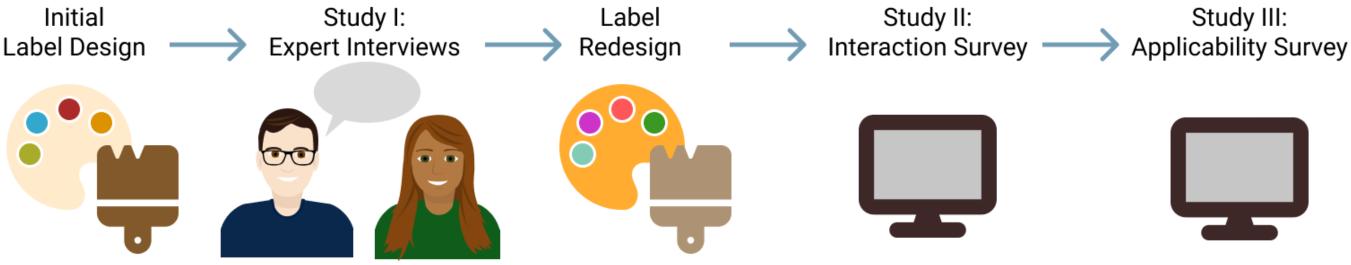

Initial Label Design
Study I: Expert Interviews
Label Redesign
Study II: Interaction Survey
Study III: Applicability Survey

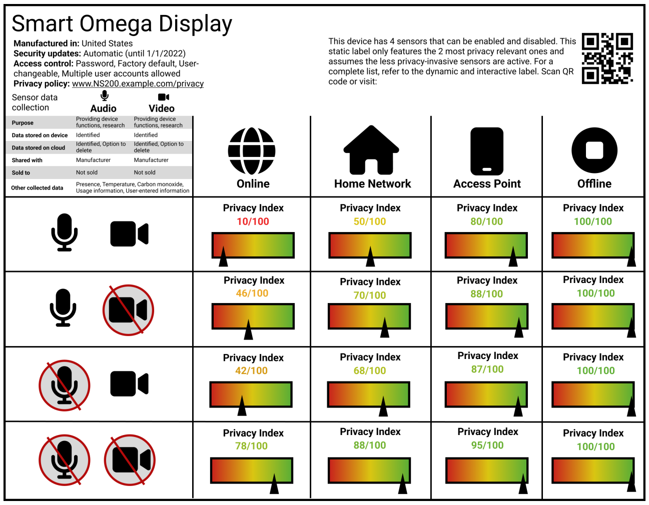
**Figure 3: Overview of our method. We first created two initial label designs, which we discussed with privacy and security experts. We then used these insights to redesign the labels and investigated how users interact with them in an online survey. Lastly, we conducted an applicability survey, investigating how well our label educates users about sensor configuration.**

participants to gather insights into the label's interpretability and usability. Finally, we conducted a second online applicability survey with 120 participants to investigate how well an interactive label educates users about sensor configuration. When advertising the surveys, we ensured that we did not mention our focus on privacy implications to avoid bias among our participants. We acquired approval from our institution's ethics board for all three studies.

## 3.1 Initial Label Design

Along with prior work [13], we designed two layers: The first layer is a static label to be printed on the device box to inform during the purchasing stage. The second layer provides more in-depth information and is reachable through a QR code. We based our designs on key insights from prior work. First, we visualize the device's impact on users' privacy [21, 28]. Aiming to use a similar metric as Jin et al. [21], we use a value ranging from 0 to 100, called the *privacy index*. To map advanced device configuration options, we reflect the device's sensor [1, 46] and connectivity [15] states. In line with prior work [15], the device's connectivity can be set to four modes: Online, local network (i.e., the device can only communicate and exchange data with other smart devices within the home and can not communicate or share data with entities outside the home over the internet), access point (i.e., the device can only communicate and exchange data with one dedicated device, such as a smartphone and can not communicate or share data with other entities or over the internet), and offline. The different sensors can be switched between two states: enabled or disabled.

The static label gives users an overview of the device's impact on privacy in combination with different configurations through a matrix visualization. In line with Emami-Naeini et al. [13] and mainly due to space limitations, we only depict the two most privacy-relevant sensors on the static label and hint at the existence of more sensors in the text next to the QR code. The code leads to the second layer of the label. Our static label design, as used in the expert interviews, can be seen in Figure 4. In contrast, the second layer of our label is an interactive website, allowing users to serendipitously explore different device configurations and directly perceive the impact on privacy, visualized with a colored slider and a numerical value. As different device configurations, especially turning sensors off or changing the device's connectivity, result in a reduced set of available features, we integrated a feature overview into the interactive label. There are two feature tables, one for the connectivity features and one for the sensor features. See Figure 5 for the interactive label design we used in the expert interviews.


Smart Omega Display

**Manufactured in:** United States
**Security updates:** Automatic (until 1/1/2022)
**Access control:** Password, Factory default, User-changeable, Multiple user accounts allowed
**Privacy policy:** www.NS200.example.com/privacy

This device has 4 sensors that can be enabled and disabled. This static label only features the 2 most privacy relevant ones and assumes the less privacy-invasive sensors are active. For a complete list, refer to the dynamic and interactive label. Scan QR code or visit:

| Sensor data collection | Audio | Video |
|---|---|---|
| Purpose | Providing device functions, research | Providing device functions, research |
| Data stored on device | Identified | Identified |
| Data stored on cloud | Identified, Option to delete | Identified, Option to delete |
| Shared with | Manufacturer | Manufacturer |
| Sold to | Not sold | Not sold |
| Other collected data | Presence, Temperature, Carbon monoxide, Usage information, User-entered information | |

| | Online | Home Network | Access Point | Offline |
|---|---|---|---|---|
| 🎤 📹 | Privacy Index 10/100 | Privacy Index 50/100 | Privacy Index 80/100 | Privacy Index 100/100 |
| 🎤 🚫 | Privacy Index 46/100 | Privacy Index 70/100 | Privacy Index 88/100 | Privacy Index 100/100 |
| 🚫 📹 | Privacy Index 42/100 | Privacy Index 68/100 | Privacy Index 87/100 | Privacy Index 100/100 |
| 🚫 🚫 | Privacy Index 78/100 | Privacy Index 88/100 | Privacy Index 95/100 | Privacy Index 100/100 |

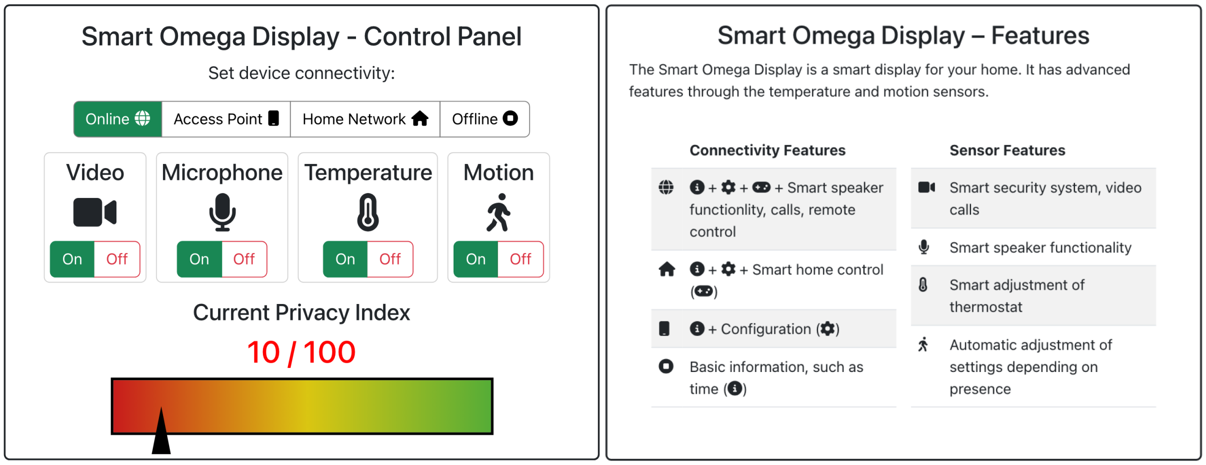
**Figure 4: Our initial *static* label for mapping advanced configuration options around device sensor state and connectivity.**

# 4 STUDY I: EXPERT INTERVIEWS

We conducted semi-structured interviews with ten privacy experts to get feedback on our initial label designs and discuss the potential of interactive labels.

## 4.1 Participants

We recruited the experts using convenience sampling, followed by snowball sampling [37]. To participate in our interviews, the experts had to match our inclusion criteria, which were to (1) self-identify as an expert and (2) pursue or have pursued a Ph.D. degree in usable privacy or a privacy-related field. Six of our ten participants identified as female and four as male. They were between 26 and 44 years old ($M = 31.1, SD = 5.3$) and had one to ten years of experience working as a privacy expert ($M = 4.4, SD = 4.3$). Five participants were PhD students, four participants were professors, and one worked as a post-doc. For a detailed overview of the experts' demographics, refer to Table 1.



Smart Omega Display – Features

The Smart Omega Display is a smart display for your home. It has advanced features through the temperature and motion sensors.

| | Connectivity Features | | Sensor Features |
|---|---|---|---|
| 🌐 | ⓘ + ⚙ + 🎮 + Smart speaker functionlity, calls, remote control | 📹 | Smart security system, video calls |
| 🏠 | ⓘ + ⚙ + Smart home control (🎮) | 🎤 | Smart speaker functionality |
| ▮ | ⓘ + Configuration (⚙) | 🌡 | Smart adjustment of thermostat |
| ● | Basic information, such as time (ⓘ) | 🚶 | Automatic adjustment of settings depending on presence |

**Figure 5: Our initial *interactive* label design.**

**Table 1: The experts' highest educational degree, current occupation, and years of experience as privacy experts.**

| PID | Education | Occupation | Exp. |
|---|---|---|---|
| E1 | Doctoral | Professor | 3 yrs |
| E2 | Master's | Ph.D. Student | 2 yrs |
| E3 | Doctoral | Post-Doc | 4 yrs |
| E4 | Master's | Ph.D. Student | 1 yr |
| E5 | Doctoral | Professor | 1 yrs |
| **PID** | **Education** | **Occupation** | **Exp.** |
| E6 | Master's | Ph.D. Student | 3 yrs |
| E7 | Master's | Ph.D. Student | 5 yr |
| E8 | Doctoral | Professor | 8 yrs |
| E9 | Doctoral | Professor | 15 yrs |
| E10 | Master's | Ph.D. Student | 2 yrs |

## 4.2 Procedure

We sent out an informed consent form and a demographics questionnaire before our interview. We conducted the interview in person or via Zoom depending on the experts' location. Before we started the recording, we ensured that our participants had signed the informed consent form and filled out the demographics questionnaire. Following Emami-Naeini et al. [13] and to set the scene for the interview, we started the conversation by asking the experts to define privacy and security in the context of IoT devices. We first introduced the concept of privacy labels for IoT devices and showed the latest labels from Emami-Naeini et al. [13] as a reference. For the primary static label, we either handed our participants a physical box with the label glued on or, in the case of online interviews, showed a picture of the box and an enlarged view of the label so that our participants could read all the detailed information. We generated the label using the official IoT label generator[2]. We asked our participants to study the label in detail while thinking aloud. After that, we instructed the experts to scan the QR code (or, in the case of online interviews, to click on the link) and repeat the same procedure for the secondary layer of the label. This first part of the interviews allowed us to create a common understanding among all participants and collect first impressions of the labels.

Next, we asked if they could imagine device configuration options that the current labels do not map. Whenever our participants had trouble developing ideas, we showed two off-the-shelf devices (one Echo Show, a smart display with a microphone and camera and one Echo Dot, a smart speaker with a microphone) to relate to current device capabilities. We then asked our participants to sketch on paper how they could imagine these configuration options to be reflected in the current labels. If the interview was remote, we asked participants to show their sketches to the camera and send us a scan of their sketches after the interview. Next, we introduced our new label designs. We started with the static label using the same procedure as the original label: We showed a physical box with the label glued on and instructed the experts to think aloud, especially focusing on the strengths and weaknesses. Afterward, we instructed our participants to follow the QR code and think aloud while interacting with the label. Whenever our participants suggested improvements, we asked them to sketch their ideas.

Finally, we discussed the opportunities enabled by interactivity and day-to-day usage of the two labels. Each interview took about one hour. We compensated participants with 10€.

## 4.3 Data Analysis

We recorded a total of 8.4 hours of audio data ($M = 50.5min$, $SD = 14.4min$) and used Atlas.ti and Thematic Analysis to systematically explore our transcripts [7]. First, two researchers open-coded two randomly selected interviews and met to discuss their codes, resolve ambiguities, and form a first joint codebook. Afterward, one researcher coded the rest of the interviews using the code book and added new codes when necessary. Finally, the two researchers met again to form groups of related codes and overarching themes. The process led to a total of 171 codes, 23 code groups, and five themes.

[2] https://www.iotsecurityprivacy.org/generate/

## 4.4 Findings

We present our findings along our five overarching themes: Static versus Interactivity, covering the perks and challenges of the different labels and discussing the opportunities enabled by interactivity, Privacy Assessment and Visualization, containing all comments about the privacy index and how it should be visualized, Feature Trade-off, describing all discussions around the importance of conveying the functionalities traded for privacy, Comparison, talking about the importance of enabling social comparisons and across products, and lastly, Integration, describing the role of the labels in users' day-to-day life. In this section, we refer to *current labels* when participants related to the privacy labels from Emami-Naeini et al. [13]. All other label references relate to our static and interactive labels.

*4.4.1 Static versus Interactivity.* This theme encompasses the experts' notions regarding the challenges and opportunities of static and interactive privacy labels. While the experts appreciated the current labels for the in-depth information they provided (E6, E10), their clear structure (E2, E10), and their focus on important aspects (E5, E9, E10), they also feared that the second layer of the label might be too complicated for laypersons (E6, E8, E9, E10) and that they might have trouble understanding the technical terms without further explanation (E1, E2, E3, E5, E6, E7, E8). Besides, the experts remarked that the current label raises concerns without offering solutions (E1, E7) and that it would be beneficial to map the device's configuration options (E1, E2, E4, E6, E7) and give estimations on whether the data practices are good or bad (E2, E3, E4, E6, E7, E8, E10): *"What exactly it would tell me as an end user, I'm not entirely sure, because again, I don't really get a rating. I don't really know if this is a good practice or a bad practice"* (E6). For both static label designs, the original and our new one, the experts noted that all sensors should be shown, not only the most privacy-relevant ones (E1, E4, E5, E7, E8, E10): *"It would make me feel a bit weird if I looked at the label, like, oh, okay, nice. And then I go in and like, oh, actually, there's a temperature sensor as well. There's a motion sensor as well"* (E7). Even though experts liked that the matrix on the new label gave an overview of all configurations and their impact on privacy (E7), they also thought the label was overwhelming (E2, E4, E9, E10) and pointed out that a matrix representation gets unfeasible as soon as more than two sensors are to be represented (E2). As a remedy, E2 suggested removing the matrix and instead displaying an impact value for each sensor. Moreover, the experts also discussed getting rid of the static label completely and instead only having a QR code on the device itself (E1, E6), as this would solve several issues, such as the label being too small to display all options (E1, E2), the label getting outdated quickly (E1), or the device box getting thrown away after purchase making the information inaccessible: *"Like I unbox my thing and then I throw it away, like immediately. I'm not keeping my boxes. So, I don't have the QR code anymore. I don't have any of the information anymore"* (E1).

In general, the experts appreciated the interactive label (E1, E2, E5, E8), as it enabled serendipitous exploring (E1, E2, E5), thus allowing users to immediately see and understand the impact of the different configurations on their privacy (E2, E4, E6, E7, E10). With this, the label might also trigger behavior change, as E6 explains: *"This might trigger people to have some sort of behavior change in the sense that they can really see the impact of what it would change if I would actually turn off the microphone."* Next to the current configuration options, the experts brought up the idea of approaching the configuration the other way around: Coming from a desired privacy index (E4, E7) or a specific use case (E2, E3, E5) and getting suggestions for the most privacy-preserving configurations, as E4 explains: *"I want to be at here, and it would give me the options of what I need to configure. So basically reverse."*

*4.4.2 Privacy Assessment and Visualization.* All experts agreed that it is important to give users the option to learn how the privacy index is calculated to ensure they can interact with the label meaningfully (E2) and interpret the value (E1, E2, E3, E5, E10): *"But since I don't understand what the index is from looking at this, I also don't really have a good feel for how bad exactly 70 out of 100 is"* (E10). Along those lines, our participants also discussed the granularity of the privacy index. While some felt a fine granularity was necessary to reflect the fine nuances between the different configurations (E1, E3, E6), others emphasized that a coarser granularity or categorization would foster understandability (E4, E5, E7, E8, E10). Suggestions to simplify the privacy index included adapting already familiar metrics, such as using letters similar to the energy or nutrition labels in Europe (E7, E8, E10) or using the traffic light metaphor with three categories (E4, E5): *"It would be helpful to have metrics also for privacy, which are similar to metrics people are already familiar with and can connect or understand better" (E10).* The experts in favor of the granular value still suggested removing the scales for the static label and instead only using colors and numbers to reduce visual clutter (E1, E2, E10). While the experts generally liked the colors for being intuitive and making the key information understandable without having to engage with the texts (E1, E2, E3, E6, E10), some raised concerns that the current color scheme might hinder accessibility across different cultures or abilities (E1, E6, E7).

*4.4.3 Feature Trade-off.* The experts emphasized the importance of informing users about the impact of the different configuration options on the available features, also on the static label (E1, E2, E3, E4, E5, E6, E7): *"They think, hey, it's really cool with the privacy index, I definitely want 100%, but then they are totally disappointed in the user experience because it just doesn't work the way it should"* (E4). Here, our experts also emphasized that the core features of a device should be marked so that the user is aware that when configuring a device in a certain way, they will not be able to use this feature anymore (E2, E9): *"What you usually distinguish is the primary functionality of that device or service or something like an addition. So, for example, if my smart fridge can sort of order food on my behalf, then if I turn off all those sensors, then the primary functionality wouldn't be there."*

The experts also suggested improvements for the interactive label's feature overview. Several experts were confused by the feature table and did not understand how the icons map to the different functionalities. Hence, they suggested using the label's interactivity by dynamically enabling and disabling the different features when adjusting settings (E1, E2, E3, E5, E10). With this, it would also be possible to map dependencies, as E3 explained: *"I turned on the video, so I could assume I can do video calls, but then again, I'm still in the offline mode, so I assume video calls will not work."*

*4.4.4 Comparison.* This theme summarizes the experts' notions about enabling cross-device (E2, E3, E4, E5, E7) and social comparisons (E2, E5). The experts discussed that the static label is too complicated to compare devices with one another (E4, E5). Instead, they recommended putting a condensed version of the privacy label on the front of the box that shows the privacy index for the device's default configuration, just like food nutrition labels in Europe (E2, E3, E4, E5, E7): *"Have it very small, just one bar at the front of the box with some standardized configuration. [...] For every smart speaker with features A-enabled, B-enabled, and C-disabled – so people are able to compare"* (E2). In regards to social comparisons, E2 and E5 suggested showing the privacy index of the average user so that people could compare themselves to others and maybe be nudged to adjust their settings: *"People will start to care more to see, okay, I'm below average. So, for example, if you see, okay, I'm now 10 from 100, and the average Alexa user has 40"* (E5).

*4.4.5 Integration.* The experts imagined how users might integrate the labels into their day-to-day routines. While E3 and E6 stated that the label might actually influence purchase decisions, they were unsure if users would revisit the interactive label to check their privacy configuration options once they finished their initial device setup (E4, E5, E6). Here, the experts suggested integrating the label into an actual control panel (E2), adding instructions on how to physically configure the device (E1, E3, E7), or sending reminders to check back on the privacy label (E3) to foster lasting engagement with the label. Notably, several participants repeatedly brought up notions of *awareness*, *education*, and *control* and discussed how the primary purpose of the labels might shift between users and at different stages of the device usage lifecycle, as E9 explains: *"So for a purchase decision, the question is, on one hand to know what the device would capture, but then also how I as a user could influence this. And then, if the device was operational, then I'd say, in the best case, it would do what I want, and I wouldn't need an interface at all. But if not, then the label should show the current state."* We find that, in particular, our interactive label sparked discussions around labels as an educational tool versus a control tool that clearly signals configuration options (E1, E2, E4, E8): *"It's very good for education and making users aware and giving them the option. But in day-to-day life, when nothing major is coming, I would not assume that the possibility of giving them actions and control and transparency will stop them from using the device and its full capabilities"* (E1).

The experts also discussed opportune moments to confront users with the label and, thus, engage with privacy tasks (E2, E7, E8, E9). E9 considered the first device set-up as such an opportune moment: *"The moment when I purchased a device, I unpack it and I first time set it up. That's when I probably sort of look at that and am willing to spare some time to engage with it."* The experts also brought up the challenge of having interactive labels in a household with many smart devices, as it would require significant effort to adjust all labels accordingly (E9): *"If I assume I have 100 smart home devices, then that would sort of create a lot of effort for me to configure this."* Lastly, the experts discussed the importance of tailoring the label to the needs of the specific target group. This was often brought up regarding the current labels as those used many technical terms, especially in the second layer, that most of the experts deemed too complex for laypersons to understand (E1, E2, E3, E5, E6, E7, E8, E9): *"I think the average user will seriously struggle with understanding what this is about because literally sort of any term that's being used on the left-hand side is something that the average user will not understand"* (E9).

## 4.5 Summary

While the experts generally liked that the new labels not only informed but also supported users in choosing more privacy-preserving options and that it provided an evaluation of the data practices by showing the privacy index, they also had suggestions for improvement. The experts stated that all sensors should be displayed on the static label and warned that the matrix adds visual clutter and gets unreasonably large with more sensors. The experts had opposing opinions regarding the privacy index. While some found the value too granular, others thought the granularity was necessary to reflect fine nuances between different configurations. In addition, the experts emphasized the necessity to explain the privacy index to make it interpretable for users. The experts greatly appreciated the interactive label for showing the immediate impact of configurations on privacy and suggested use case interactions where users define a specific scenario or a desired privacy index and get suggestions on how to configure their devices. Along those lines, the experts also emphasized the importance of visualizing the features getting traded in favor of privacy. They also suggested joining the two tables in the interactive label to visualize the interdependency of connectivity and sensor features. Moreover, the experts proposed making the features interactive along with user configurations. Finally, most experts believed that the label would support users mainly during the purchasing stage and that it might presume different roles during the device's lifecycle: It might serve as an awareness, educational, or control tool.

## 4.6 Label Redesign

The experts found the *interactive* label to be the most interesting as it enabled new forms of interaction. Along with the experts' comments, we merged sensor and connectivity features and made them dynamic: When users change sensor or connectivity states, the respective features get grayed out or highlighted in green. See Figure 1 for our reworked interactive label design. As several experts questioned the suitability of the static label to reflect advanced configuration options, we decided to adapt only the design of the *interactive* label for further evaluation. Based on several expert remarks, we added the following explanation for the calculation of the privacy index:

A higher privacy index indicates less exposure to privacy risks. It is calculated based on the following four factors:

(1) Sensor Type: Each sensor type has a value depending on its impact on users' privacy. Example: Since a video camera records more personal data than a motion sensor, it has a stronger negative impact on the privacy index.
(2) Sensor Specifications: The technical specifications of a sensor impact the privacy index calculation. For example, a video camera filming in wide-range 4K resolution is more privacy-sensitive than a 780p low-resolution camera.
(3) Device Connectivity: A device that is online and has the potential to share data with other entities has a bigger negative

impact on the users' privacy than an offline device that can not share data with other entities.

(4) Device Specific Factor: We consider publicly available vulnerability reports for entries about the specific device. Sometimes, a device or a certain firmware version, for example, is especially prone to security vulnerabilities. This pillar specifically considers device security.

# 5 STUDY II: ONLINE SURVEY

Next, to determine how users perceive the interactive labels and gather insights into their interoperability and usability, we conducted an online survey on Prolific ($N = 160$).

## 5.1 Survey Construction

We first asked the participants to complete the IUIPC questionnaire [29] to understand their general perception of privacy before instructing them to complete the four tasks described in the following. To ensure the data quality, we saved a timestamp after each task and used an attention check item; refer to Appendix A for the complete questionnaire. The four tasks aimed at the usability of the interactive label through the four key research challenges found in Study I: Privacy awareness versus simple control (Task 1), feature and privacy trade-off (Task 2), and use-case-based label configurations (Tasks 3 and 4).

*5.1.1 Task 1.* Aiming to investigate the effect of the different interface elements, we conducted the first task between subjects so that every participant only saw one condition. We visualize the different conditions in Figure 1: The Only Control condition used UI element (1), the Control × Privacy Index condition used elements (1) + (2), the Control × Features conditions used elements (1) + (3), and the last condition, Control × Privacy Index × Features, used elements (1) + (2) + (3). All subsequent tasks used the Control × Privacy Index × Features condition.

In the first task, we asked our participants to immerse themselves in a situation where they bought a smart display with a QR code on the box leading to a website. Then, we asked our participants to use the website to configure the device's sensors and connectivity according to their preferences and explain their configuration choices in at least one sentence. Afterward, we asked them to rate their agreement to three statements on 100-point sliders ranging from Strongly disagree to Strongly agree. We favored visual analog scales (VAS) instead of Likert scales, as they lead to more precise responses, higher data quality [17], and collect continuous data, which allows for more statistical tests [38]. We also did not use ticks to prevent the responses from converging around those [32]. Our statements asked whether the website supported our participants in making an informed decision and whether the device's features or privacy were the most influential factors when configuring their device. Additionally, we also saved their exact configurations.

*5.1.2 Task 2.* Next, we confronted our participants with screenshots of the interactive labels of three slightly different smart displays. The Smart Omega Display had a privacy index of 55 and only a few features; the Smart Gamma Display had a privacy index of 22 and more features than the Omega display, and the Smart Alpha Display had a privacy index of 5 and the most features. Then, we asked our participants in a multiple-choice task to select the display they would be most likely to buy and to describe the factors influencing their purchase decision. This task tackles feature and privacy tradeoffs as well as device comparison.

*5.1.3 Tasks 3 and 4.* Lastly, we investigated whether our participants understood how the label could be configured. These tasks are inspired by the experts imagining use-case-based interactions with privacy labels. For this, we confronted our participants with two concrete situations, asked them to configure the label accordingly, and finally, to enter the resulting privacy index. In the third task, we investigated the configuration of the sensor states using the following description: *"A user owns two Smart Beta displays. 1) The user wants both devices to be able to always react to voice commands. 2) The user also wants to be able to do calls on both devices. However, only the device in the kitchen should allow video calls. The device in the bathroom should not allow access to the camera."* The fourth task builds upon the third, asking the participants to consider the device's connectivity: *"The user's partner does not like the fact that the devices could send data across the internet. However, the partner does like to use the "Advanced configuration" and "Limited remote access within home" features. Configure the label accordingly."*

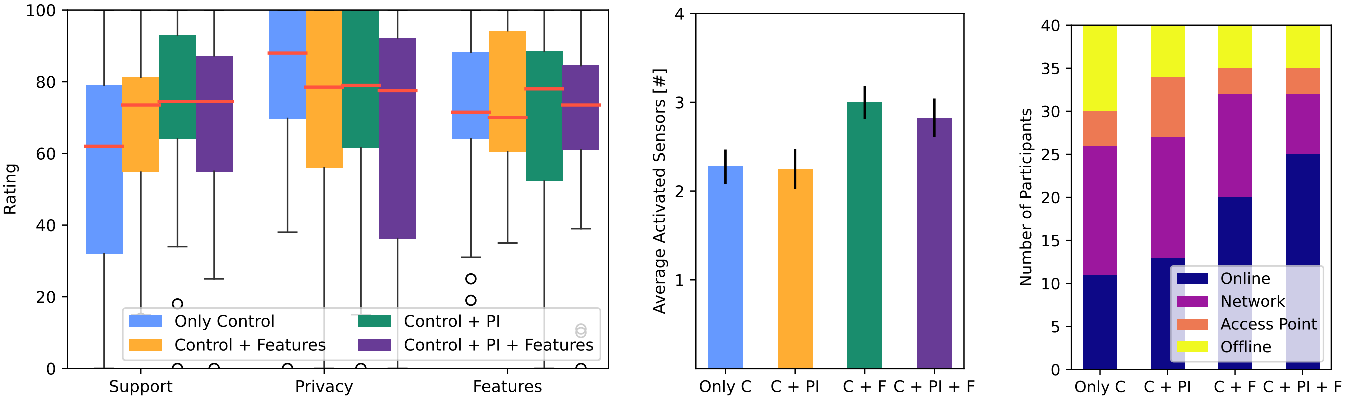
## 5.2 Participants

We recruited 160 participants, meaning each condition in task 1 was completed by 40 participants. We recruited our participants in several batches to counterbalance our sample regarding gender and country and to replace participants who failed our attention check (4) or intentionally gave low-effort responses (1). Our participants were between 21 and 67 years old ($M = 33$, $SD = 8.9$); 84 identified as male, 73 as female, and three as non-binary. The participants were from 39 different countries, with most (15) stemming from Portugal, Greece (13), South Africa (12), the United Kingdom (12), and Mexico (11). Most (59) held an undergraduate degree, 58 a graduate degree, and 20 a high school diploma. We employed the IUIPC questionnaire using a 7-point Likert scale (higher scores indicating higher privacy levels) to measure the participants' general perception of privacy. The sample had an average score of 6.2 ($SD = .9$) for Awareness, 5.7 ($SD = 1$) for Control, and 5.7 ($SD = 1.1$) for Collection, which indicates rather high levels of privacy concerns for all three areas when employing a similar interpretation as prior work (c.f., [20]). The survey took approximately 8 minutes, and we compensated our participants with 1.2£.

## 5.3 Results

We used Python and R to analyze our quantitative data and thematic analysis [7] to make sense of our participants' qualitative survey responses. We used Dunn's test with Holm-Bonferroni corrections as post hoc tests for all significant results.

*5.3.1 Task 1: Configuration Preferences.* We first investigated which condition our participants' found to support them best in making an informed decision. As our data were not normally distributed ($W = .934$, $p < .001$), we used a Kruskal-Wallis test which revealed significant differences ($p < .05$). Pairwise post hoc tests showed that the Control × Privacy Index condition supported our participants significantly better in making an informed decision than having



**(a) Boxplots showing our participants' ratings regarding their perceived support (*Support*) and whether *Privacy* or the *Features* were the most influential factors during configuration.**

**(b) Bar charts showing how many sensors participants activated on average by condition.**

**(c) Stacked bar charts showing the configured connectivity by condition.**

**Figure 6: Visualization of the results from task 1. *PI* refers to conditions in which the *Privacy Index* was shown.**

the Only Control condition. We did not find any significant differences between the conditions regarding whether the features or privacy considerations were the most influential factors when configuring the devices; see Figure 6a.

Additionally, we investigated how our participants configured their devices; see Figure 6b and Figure 6c. First, we investigated differences in the configured sensors. As our data was once again not normally distributed ($W = .85$, $p < .001$), we used a Kruskal-Wallis test which revealed significant differences ($p < .05$). Yet, pairwise post hoc tests showed no significant differences. Yet, we see that while participants in the Only Control condition activated 2.28 sensors and 2.25 sensors in the Control × Privacy Index on average, participants in the Control × Features condition activated three sensors, and participants in the Control × Privacy Index × Features 2.82. This shows that visualizing the features' impact while configuring led to participants activating more sensors.

Next, we investigated the connectivity configurations. Once again, our data was not normally distributed ($W = .63$, $p < .001$). A Kruskal-Wallis test revealed significant differences ($p < .01$) between the conditions and pairwise post hoc tests showed that participants in the Control × Privacy Index × Features condition kept their device's significantly more often in online mode than participants in the Control × Privacy Index ($p < 0.05$) and Only Control ($p < 0.01$) conditions. Again, this shows that directly communicating the impact of connectivity configurations on device features resulted in a shift from increased privacy to an increased number of features.

Our qualitative data helps explain the configuration choices. Here, 25 participants stated having only considered their privacy when configuring their devices. Looking at the differences by condition, we see eight participants in the Control × Privacy Index and nine in the Only Control made that statement. Yet, only six participants in the Control × Privacy Index × Features condition and two participants in the Control × Features said privacy was their most influential factor. This can explain why participants in these conditions activated more sensors on average. Moreover, 35 participants stated they based their configuration on the best privacy-feature trade-off. Yet, when looking at the codes by condition, we see that ten participants in the Control × Features, ten in the Only Control, nine in the Control × Privacy Index × Features condition, but only six in the Only Control condition made that statement. This makes sense as this condition does not visualize the device's features or impact on privacy and, thus, does not provide much guidance on making a trade-off decision.

In summary, we found that having the privacy index available made participants feel significantly better supported in making configuration choices than having only the control panel available. In addition, we found that showing the impact of configurations on the available feature set led to participants activating more sensors and keeping them in online mode more frequently.

### 5.3.2 *Task 2: Purchase Decisions.*

Most (121) participants chose the smart display with the highest privacy index and the least amount of features, 22 chose the one with the medium privacy index and the medium amount of features, and 17 chose the display with the low privacy index and the most features. When asked to justify their choice, most (103) stated having decided solely based on the privacy index (103), as P47 explains: *"The privacy index was pretty much my sole reason for choosing what I did. The higher the score, the safer it made me feel."* In contrast, 37 participants stated having based their decision on the best privacy-feature trade-off: *"A good balance between privacy and features. The omega has too few features to be useful for anything while the alpha just knows too much"* (96). Moreover, 20 participants stated that the additional features were not worth giving up on privacy, and 17 stated that they decided solely based on the available features.

### 5.3.3 *Task 3 and 4: Configuring a Device According to Description.*

In task 3, we asked participants to configure one smart display for the kitchen and one for the bathroom. Both were supposed to be able to do calls, but only the one in the kitchen should allow video calls, meaning participants should keep both devices in online mode and the microphone enabled while also disabling the video sensor for the device placed in the bathroom. Overall, 70% configured the device for the kitchen correctly and 70.6% for the bathroom. While the minimal correct option for the kitchen was a privacy index of 10 (i.e., no configurations but keeping the connectivity and sensors in default state), 45.5% of the 112 participants who solved the task correctly chose a more privacy-preserving variant. The same was true for the bathroom, where 64.3% of the correct answers resembled a more privacy-preserving configuration.

Task 4 required participants to configure the display so that it is not connected to the internet but still has the "advanced configuration" and the "limited remote access within the home" features available. This task was completed correctly by 65% of all participants, whereby 29.8% additionally deactivated sensors, even though the task only required the participants to set the connectivity to the "local network."

Overall, we found that most participants chose the device with the highest privacy index when asked to make a purchasing decision and that most participants understood the interaction with the label, as they configured it correctly according to the task descriptions.

### 5.4 Summary

We conducted an online survey to determine how users interact with the labels. We found that having the privacy index available made participants feel significantly better supported in making an informed decision on configuring their devices than having only the control panel available. Moreover, we found that most participants would choose the device with the highest privacy index during purchasing decisions. Lastly, we found that our participants understood the label's configuration options, as most participants configured the devices correctly according to our text descriptions.

## 6 STUDY III: APPLICABILITY ONLINE SURVEY

Lastly, to find out how well our interactive privacy label educates users about sensor configuration (**RQ3**), we conducted an applicability survey. In detail, we investigated (1) how important users perceive the information provided by the label, i.e., learning about the different device sensors, their privacy impact, and deactivation options, and (2) whether users currently face issues when trying to retrieve this information and if our interactive label succeeds in educating users. To answer these questions, we conducted a second, between-subject online survey.

### 6.1 Survey Construction

As we wanted to determine whether users currently face issues learning about smart devices, we needed to compare the existing informing methods with our newly developed privacy label. Therefore, we implemented a between-subject design with three conditions: The current official Product Page of a smart device, the Established Label by Emami-Naeini et al.'s [13] generated using the official label generator [3] and our newly developed Interactive Label. We slightly adjusted our label and removed the parts that are not yet integrated into smart devices, i.e., the privacy index and the connectivity modes *local network* and *access point* as we wanted the label to accurately reflect the reality to ensure comaprability. We selected three smart devices for our online survey: The Google Nesthub 2nd generation, the Amazon Echo Show 8 3rd generation, and the Apple Homepod 2nd generation. We chose these devices as they were among the top smart speaker models at the time of writing this paper, came from different manufacturers, and, thus, had different product pages, and they all had the same core functionality while offering slightly different feature sets.

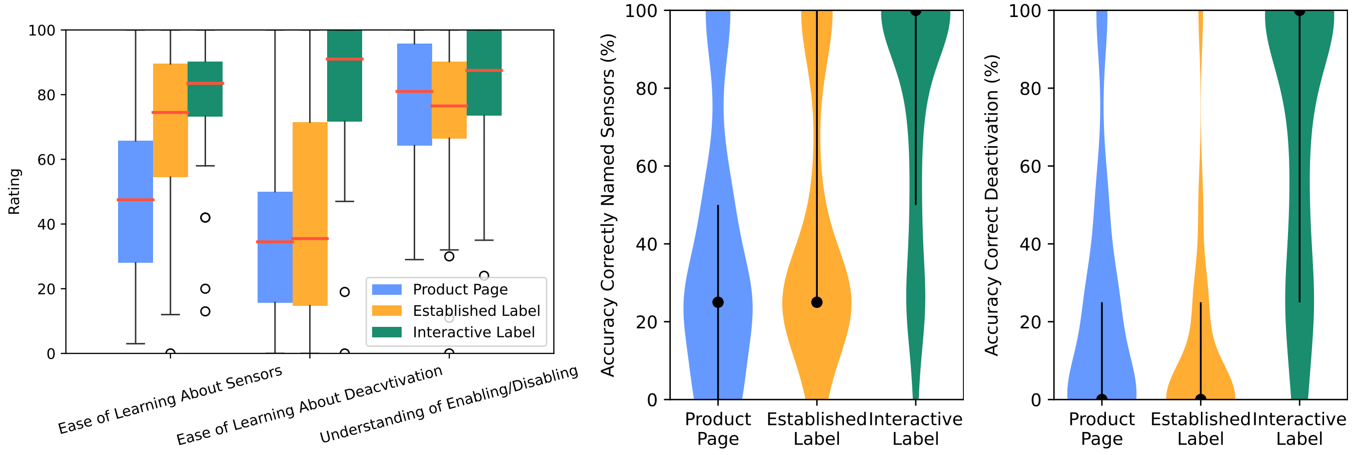
After answering the IUIPC questionnaire [29], we presented all three smart devices in random order. We asked the participants to engage with the displayed information thoroughly (depending on the condition, the official product page, the established privacy label, or our interactive label – for the two privacy labels, we also added a picture of the device to give the participants a visual hook) and then proceed to the questions. We also advised our participants that they were free to revisit the information while answering the questions at any time. The following questions were repeated until the participant declared that the device had no more sensors. We first asked the participants to name one individual sensor of the current smart device via a free text field. We then asked them which of the following statements was true: *The device allows me to disable the sensor* or *the device does not allow me to disable the sensor.*

After these questions, we asked our participants to rate their agreement to six statements using the same sliders as before. The statements appeared in random order and asked about the perceived **importance** of learning (1) which sensors a device has, (2) whether those sensors are deactivatable, and (3) about the privacy implications of these sensors. Next, we asked how **easy** participants found it to find information about (4) the installed sensors and (5) their deactivation options. Finally, we asked if the participants (6) understood the consequences of deactivating sensors on the device behavior. The exact wording of these statements and the full questionnaire can be found in Appendix B. We further contribute the privacy labels we used for our survey, which we created based on publicly available information and which were validated by two researchers, see **??**.

### 6.2 Participants

We recruited 120 participants (i.e., 40 per condition) in several batches to counterbalance the sample in terms of gender and country and to replace participants who either faced technical problems because they had JavaScript disabled (2) or intentionally gave low-effort responses, such as stating that a device did not have a single sensor (3). Our participants were between 18 and 64 years old ($M = 34$, $SD = 10$); 58 identified as male, 59 as female, and three as non-binary. The participants were from 41 different countries, with most (8) stemming from Turkey, Spain (8), Greece (6), Portugal (6), and the United Kingdom (6). Most (43) held a graduate degree, 40 had an undergraduate degree, and 17 had a high school diploma. We used the IUIPC questionnaire using a 7-point Likert scale (higher scores indicating higher privacy levels) to gauge the participants' general perception of privacy. The participants had an average score of 6.1 ($SD = .9$) for Awareness, 5.5 ($SD = 1.1$) for Control, and 5.6 ($SD = 1.1$) for Collection, reflecting a rather high level of privacy concerns across all three areas (following the interpretation from Hoyle et al. [20]). The participants spent approximately 11 minutes on the survey and were compensated with 1.65£.

[3] https://www.iotsecurityprivacy.org/generate/



**(a) Boxplots showing how easily participants learned about (1) available sensors, (2) their deactivation options, and (3) if they understood the impact of enabling or disabling sensors.**

**(b) Violin plots showing the accuracy of participants' responses regarding correctly identified sensors per device.**

**(c) Violin plots showing the accuracy of participants' responses regarding whether a sensor could be deactivated.**

**Figure 7: Box and violin plots showing how well the conditions performed regarding different measurements.**

## 6.3 Results

We used Python and R to analyze the survey data. We report our results along the two questions of (1) gauging the participants' perceived importance of sensor information and (2) finding out whether users currently face issues when retrieving sensor information and if our label provides a remedy. We again used Dunn's test with Holm-Bonferroni corrections as post hoc tests for all significant results.

*6.3.1 Importance of Sensor Information.* We first investigated how important participants perceived it to learn about (1) which sensors a smart device has, (2) how these sensors can be deactivated, and (3) what impact these sensors have on users' privacy. Our findings show that all three dimensions were rated as important, with medians of 86 for sensor knowledge ($M = 79.79$, $SD = 21.85$), 87 for deactivation knowledge ($M = 79.69$, $SD = 22.32$), and 84 for knowledge on the privacy impact ($M = 78.88$, $SD = 21.74$).

*6.3.2 Retrieving Sensor Information by Condition.* Next, we investigated if users currently face issues when informing themselves about smart devices and if users perform better using our newly developed INTERACTIVE LABEL. For this, we first focused on subjective measures and investigated how easy users found it to retrieve (1) sensor information, (2) information about deactivation options, and (3) whether they felt they understood the impact of disabling sensors on the device functionality. The INTERACTIVE LABEL received the highest ratings across all three statements; see Figure 7a. Next, we investigated the accuracy of (4) correctly named sensors and (5) correctly identified deactivation options. Figure 7b and Figure 7c show that also here the INTERACTIVE LABEL performed best.

**Ease of Learning about Sensors.** As our data was not normally distributed ($W = .93$, $p < .001$), we used a Kruskal-Wallis test, which revealed significant differences ($p < .001$), and pairwise post hoc tests showed that participants found it significantly easier to find information about the available sensors using the INTERACTIVE LABEL compared to the PRODUCT PAGE ($p < .001$) and significantly easier using the ESTABLISHED LABEL compared to the PRODUCT PAGE ($p < .05$). The difference between the INTERACTIVE LABEL and the ESTABLISHED LABEL was not significant.

**Ease of Learning about Sensor Deactivation.** Since the data was again not normally distributed ($W = .9$, $p < .001$), we used a Kruskal-Wallis test that revealed significant differences ($p < .001$) between the conditions. Pairwise post hoc tests showed that participants found it significantly easier to find information about deactivating the sensors using the INTERACTIVE LABEL compared to the PRODUCT PAGE ($p < .001$) and ESTABLISHED LABEL ($p < .001$).

**Understanding Impact of Sensor Deactivation.** Again, the data was not normally distributed ($W = .87$, $p < .001$). A Kruskal-Wallis test revealed no significant differences ($p = .24$).

**Accuracy of Correctly Named Sensors.** The data was not normally distributed ($W = .8$, $p < .001$). Thus, we conducted a Kruskal-Wallis test, which revealed significant differences ($p < .001$). Pairwise post hoc tests showed that participants listed significantly more correct sensors using the INTERACTIVE LABEL compared to the ESTABLISHED LABEL ($p < .001$) and the PRODUCT PAGE ($p < .001$).

**Accuracy of Correctly Identified Deactivation Options.** Since the data was not normally distributed ($W = .75$, $p < .001$), we used a Kruskal-Wallis test, which revealed significant differences ($p = .001$). Pairwise post hoc tests showed significant differences between all conditions. Participants had a significantly higher accuracy using the INTERACTIVE LABEL compared to the PRODUCT PAGE ($p < .001$) or Established Label ($p < .001$), but the participants also had a higher accuracy using the PRODUCT PAGE compared to the ESTABLISHED LABEL ($p < .05$).

In summary, the participants found all information conveyed in the label important. Moreover, participants retrieved sensor information more easily and effectively with the interactive label.

# 7 DISCUSSION

We presented the design process of our privacy labels, detailed how they were impacted by findings from our expert interview study ($N = 10$), and reported the results from an online usability ($N = 160$) survey and applicability survey ($N = 120$). In this section, we discuss the sum of findings from the studies through the lenses of our three research questions.

## 7.1 RQ1: How can we reflect advanced smart device configuration options in privacy labels?

The academically and politically well-received IoT privacy and security labels designed and evaluated by Emami-Naeini et al. [13, 14] set the scene for systematically communicating smart device features and privacy risks. Our findings from Study I showed that privacy and security experts consider them highly valuable and thorough. Yet, the participating experts also stressed that the information level provided by these labels, particularly the second layer label, might be too complicated for laypersons. This is particularly interesting concerning mapping additional smart device configuration options like sensor control [46] and the control of device connectivity [15, 21] as those require integrating even more information. As a result, we find that **new interaction and visualization techniques must be explored to reflect advanced smart device configuration options**.

One visualization option relates to icons and visual metaphors that most consumers are familiar with. In fact, the first label from Emami-Naeini et al. [14] featured two 5-star ratings. The authors removed those star ratings in their label designs later [13], arguing that to date, no independent rating agencies existed that would allow performing these assessments. However, they highlighted that such a metric would be important to enable users to compare devices. In the context of our work, we note that **enabling comparability in even more complex device configuration scenarios necessarily requires quantifiable measures and easy-to-understand data representations**. This, in turn, requires establishing trustworthy assessment criteria and independent rating agencies. In fact, prior work has already shown that manufacturers exploit labeling schemes. For example, in the context of EU energy consumption labels, manufacturers intentionally misreported their energy consumption to appear more energy-efficient than they truly were [19]. At the same time, consumers reported trusting more in mandatory environment labels as those are usually authenticated by independent third parties [42]. Consequently, we stress that, when employed in practice, **indicating a device's privacy impact must be mandatory and authorized by independent third parties to ensure their truthfulness and user trust.**

While such infrastructure has yet to be established, we can provide a foundation for future labels by empirically evaluating visualizations that enable device comparability. In our case, we initially used sliders in a matrix for the static label before realizing in Study I that they were too complex. In fact, the experts asked for simpler metrics and visualizations on the static label or even argued for dropping the static label completely in favor of a QR code that links to the interactive label. In contrast, they largely appreciated the privacy index of the interactive label that we refined in our final interactive label design. Yet, our findings also show that future **iterations of visualizations like the privacy index must consider interpretation intuitiveness, granularity, and expectation management**. In particular, sticking to a fine-grained representation like the current 100-point privacy index slider requires communicating to users that a score close to 100 might not be reachable in case of feature-heavy use and that lower scores might very well be acceptable. As such, **fine-grained representations are likely to shift the main purpose of quantifiable measures and visualization from creating basic assessments for awareness (like stars) to in-detail comparability of devices.** We argue that this shift might very well be necessary given the vastly increasing number of smart home devices and increasingly complex device configuration options. In this context, we also note the immense responsibility of visualizing such fine-grained assessments. In the second task of our survey study, 121 participants chose the smart display with the highest privacy index, with 103 stating that they *solely* decided based on the privacy index. This is also partially reflected in the third and fourth tasks, where 45.5% and 29.8% of participants chose more privacy-preserving configurations than the task requested. Yet, these results should also be considered cautiously: While a device might appear privacy-threatening at first due to a low privacy index, it might be highly configurable, leading to an easily increasable privacy index without losing much of the promised feature set. **This trade-off between helping users make informed purchasing decisions and deterring users from purchasing devices solely because their initial privacy index might be low must be considered by future research on privacy quantification.** A possible solution is to display a range instead of a fixed value to indicate that a device's privacy impact is not fixed but varies depending on the settings.

## 7.2 RQ2: What role does interactivity play in the design of advanced privacy labels?

We initially designed one static and one interactive label but found in Study I that accurately reflecting advanced device configuration options in a static label is challenging, if not unfeasible. In fact, Emami-Naeini et al. [14] also discussed the downsides of static labels: *"The rapid pace at which IoT devices receive software and firmware updates could make it a challenge for manufacturers to keep their labels up to date."* The authors discussed as a *"realistic solution (...) to have labels marked with software and hardware version numbers, with QR codes or hyperlinks to the label for the latest firmware"*. However, reviewing the latest computer security research on smart devices, we note that vulnerabilities and countermeasures are subject to such a high level of fluctuation in a dynamic space that static labels will frequently be outdated or even misleading. This understanding is particularly well reflected in the work of Oser et al. [36], who present an automated and scalable framework for IoT device scoring. Since device security is one of the envisioned assessment pillars for our privacy index and is further reflected in the current IoT privacy and security labels [13, 14], we argue that the value and use of static labels should be subject to further investigation. Combined with limitations in reflecting advanced device configuration options, this **leads to questions about the usefulness and role of the static or primary label layer**. Indeed, the printed label on product packages might actually just contain a QR code linking to the online version of the label and contain, at most, very basic information like an overview of the types and sensors installed and their physical configurability.

However, **we note that a novel type of interactive label also raises interaction challenges around usability and accessibility**. Navigating through a QR code to an interactive label requires a minimal skill set and physical abilities that could potentially exclude some of society. Windl et al. [46] related their research on tangible smart device sensor control to inclusiveness, stressing that tangible control mechanisms contribute to *inclusive privacy*. In the label context, we note that **the shift towards an interactive label requires designers and manufacturers to place particular emphasis on the accessibility of this transition**. Options might include printing large QR codes for the elderly, visually impaired, or motor impaired users; built-in RFID tags that open the interactive label website automatically; and dedicated support hotlines that guide towards the interactive label.

Regarding label usability, we note that *interactive* labels that provide actual configuration options, rather than just informative tooltips, are not widely used and are unfamiliar to most users. One exception is *Healthy Shelf*, an interactive nutrition label that calculates nutrition values based on custom serving sizes and features a comparison between two products [6]. The label designers motivate their work largely through findings of Rothman et al. [39], who report on a survey study with 200 participants who were asked to calculate the number of carbohydrates for a specific serving size. The authors found that only 37% of the participants could answer correctly. In contrast, in the preliminary evaluation of *Healthy Shelf* with nine participants, the six tasks were completed with an accuracy between 50% and 100%. In contrast, our survey Study II with 160 participants reports on a much wider usability evaluation of *interactive* labels. While we note that privacy labels are way less common than nutrition labels, the successful completion rate of the use-case-based configuration tasks 3 and 4 were 70.6% and 64.3%, respectively. Given the lack of familiarity with *interactive* labels in general and privacy labels specifically, we consider those results as a promising starting point. Yet, we note that **researchers and designers of *interactive* labels will need to continue observing and improving the usability of this novel information tool in the context of IoT privacy and beyond**.

One of the main discussion points in the expert Study I related to the primary use of the *interactive* labels. Almost all noted that the labels are suitable to create *awareness* for data privacy and that they help *educate* consumers. Yet, several experts also discussed a **possible shift of primary label use from static to interactive label towards *control***. They noted that manipulating the device state on the label would likely advocate for an actual state change in the smart device. In this context, some experts further discussed how consumers would approach the interactive labels. While the current labels are mostly designed to create an overview of key characteristics during device purchase and use, the experts envisioned that the interactive label might be used for concrete use cases. We designed tasks 3 and 4 to reflect such realistic scenarios and found that most users could use the labels directly. Still, we stress that **this novel form of label interaction must be further evaluated in the wild to profit from lived experiences**.

## 7.3 RQ3: How well does an interactive privacy label educate users about sensor configuration?

We designed our interactive labels based on the requirements of an evolving smart device landscape marked by increasingly diverse sensors and configuration options. Aiming to reflect these novel developments, we designed interactive labels that, on the one hand, clearly communicate the device's sensors and their states but that are also configurable to reflect the impact of deactivating sensors on the device's privacy and feature set. Yet, having such labels while users do not perceive the provided information as important or if they fail to make finding information easier and more accurate would make them redundant. Hence, our third study investigated whether the labels successfully educated users about sensor configuration. Our results showed that participants considered all aspects of the interactive label highly important. This implies that users actually **want to learn about the different sensors, whether they can deactivate them, and what impact they have on their privacy.** Our participants also perceived interacting with the interactive labels to retrieve information about sensor types and deactivation options significantly easier than with the currently available options. Further, our participants could name device sensors and deactivation options significantly more accurately using our interactive labels. In contrast, the product page and established label were insufficient in communicating this information, which is reflected in the fact that users could barely name the sensors correctly or decide if they were configurable. Hence, **we call future researchers and especially device manufacturers to include this information prominently to allow users to make informed decisions about smart device purchase and usage.**

## 7.4 Limitations and Future Work

We used an online survey to investigate how users interact with interactive privacy labels. While we argue that this method successfully provided us with the first important insights, online surveys might result in participants indicating answers that do not reflect their actual behavior [23]. During real-life purchase decisions or when already having a smart device at home, the convenience granted by a large feature set might outweigh privacy considerations. Hence, it will be important to repeat our investigation in a more naturalistic setting, for example, by equipping smart homes with configurable devices and labels through a long-term in-the-wild study. This will provide in-depth insight into users' perceptions around information validity, transparency, and the role of independent third parties in authenticating these privacy assessments. These are important next steps on the path to broad real-world use.

Most of our interviewed experts came from Germany, and most of our survey participants were from the Western population. This must be acknowledged, as these populations tend to have very strong views on privacy protection [40], which might have skewed our findings. Hence, we argue for future research across diverse populations to ensure the generalizability of our findings.

A potential pitfall of equipping smart home devices with privacy labels, especially in combination with quantified privacy scores, is that users might fail to interpret them correctly. In fact, such behavior was found in regard to energy consumption labels, where users misinterpret the labels, which ultimately led to worse purchasing decisions than without the label [43]. This shows the importance of designing the label carefully and educating users about the correct interpretation before deploying them in the wild.

Finally, the experts discussed how the label's role might change over time. While it will most likely serve as an educational tool to support users during the purchasing stage, it might evolve into an awareness tool as users use it to check back on their device configurations. Moreover, our experts suggest evolving the label into a control tool so that the configurations have a real-life impact on the device's settings. We encourage future research to explore this broad potential of interactive privacy labels further to ensure a lasting positive impact.

## 8 CONCLUSION

We conducted three studies to understand the potential of interactive privacy labels. Based on extensive prior research, we created novel IoT privacy label designs focusing especially on mapping advanced device configuration options and conveying the device's privacy impact via a score. We refined the labels through our expert interview study ($N = 10$) before we evaluated them for their interpretability and usability in a large-scale online survey ($N = 160$). Finally, we conducted a second online survey ($N = 120$) to investigate how well the labels educate users about sensor configuration. We found that mapping advanced configuration options calls for interactive digital labels compared to static ones. Moreover, we found that users successfully interpreted our labels and retrieved sensor information more efficiently and correctly, and oftentimes, they chose more privacy-preserving options than required.

## REFERENCES

[1] Imtiaz Ahmad, Rosta Farzan, Apu Kapadia, and Adam J. Lee. 2020. Tangible Privacy: Towards User-Centric Sensor Designs for Bystander Privacy. *Proc. ACM Hum.-Comput. Interact.* 4, CSCW2, Article 116 (oct 2020), 28 pages. https://doi.org/10.1145/3415187

[2] Bayan Al Muhander, Jason Wiese, Omer Rana, and Charith Perera. 2023. Interactive Privacy Management: Toward Enhancing Privacy Awareness and Control in the Internet of Things. *ACM Trans. Internet Things* 4, 3, Article 18 (sep 2023), 34 pages. https://doi.org/10.1145/3600096

[3] Noah Apthorpe, Dillon Reisman, and Nick Feamster. 2016. A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic. *Workshop on Data and Algorithmic Transparency* (2016).

[4] Natã M Barbosa, Joon S Park, Yaxing Yao, and Yang Wang. 2019. "What if?" Predicting Individual Users' Smart Home Privacy Preferences and Their Changes. *Proceedings on Privacy Enhancing Technologies* 2019, 4 (2019), 211–231. https://doi.org/10.2478/popets-2019-0066

[5] Susanne Barth, Dan Ionita, and Pieter Hartel. 2022. Understanding Online Privacy—A Systematic Review of Privacy Visualizations and Privacy by Design Guidelines. *ACM Comput. Surv.* 55, 3, Article 63 (feb 2022), 37 pages. https://doi.org/10.1145/3502288

[6] Sapna Bedi, Javier Diaz Ruvalcaba, Zoltan Foley-Fisher, Noreen Kamal, and Vincent Tsao. 2010. Health Shelf: Interactive Nutritional Labels. In *CHI '10 Extended Abstracts on Human Factors in Computing Systems* (Atlanta, Georgia, USA) *(CHI EA '10)*. Association for Computing Machinery, New York, NY, USA, 4405–4410. https://doi.org/10.1145/1753846.1754161

[7] Ann Blandford, Dominic Furniss, and Stephann Makri. 2016. *Qualitative HCI Research: Going Behind the Scenes.* Morgan & Claypool Publishers, 51–60. https://doi.org/10.2200/S00706ED1V01Y201602HCI034

[8] Joseph Bugeja, Andreas Jacobsson, and Paul Davidsson. 2016. On privacy and security challenges in smart connected homes. In *2016 European Intelligence and Security Informatics Conference (EISIC, 16)*. IEEE, 172–175. https://doi.org/10.1109/EISIC.2016.044

[9] George Chalhoub, Martin J Kraemer, Norbert Nthala, and Ivan Flechais. 2021. *"It Did Not Give Me an Option to Decline": A Longitudinal Analysis of the User Experience of Security and Privacy in Smart Home Products.* Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3411764.3445691

[10] Yuxin Chen, Huiying Li, Shan-Yuan Teng, Steven Nagels, Zhijing Li, Pedro Lopes, Ben Y. Zhao, and Haitao Zheng. 2020. Wearable Microphone Jamming. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3313831.3376304

[11] Eun Kyoung Choe, Sunny Consolvo, Jaeyeon Jung, Beverly Harrison, Shwetak N. Patel, and Julie A. Kientz. 2012. Investigating Receptiveness to Sensing and Inference in the Home Using Sensor Proxies. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing* (Pittsburgh, Pennsylvania) *(UbiComp '12)*. Association for Computing Machinery, New York, NY, USA, 61–70. https://doi.org/10.1145/2370216.2370226

[12] Youngwook Do, Jung Wook Park, Yuxi Wu, Avinandan Basu, Dingtian Zhang, Gregory D. Abowd, and Sauvik Das. 2022. Smart Webcam Cover: Exploring the Design of an Intelligent Webcam Cover to Improve Usability and Trust. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 5, 4, Article 154 (dec 2022), 21 pages. https://doi.org/10.1145/3494983

[13] 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.

[14] 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.

[15] Sebastian S Feger, Maximiliane Windl, Jesse Grootjen, and Albrecht Schmidt. 2023. ConnectivityControl: Providing Smart Home Users with Real Privacy Configuration Options. In *International Symposium on End User Development*. 180–188.

[16] Gert Franke, Thomas Clever, Wouter van Dijk, Jeremy Raider, and Roel de Jonge. 2019. *Privacy Label.* https://medium.com/sensor-lab/the-privacy-illusion994ed98ec3ab Retrieved December 10, 2019.

[17] Frederik Funke and Ulf-Dietrich Reips. 2012. Why Semantic Differentials in Web-Based Research Should Be Made from Visual Analogue Scales and Not from 5-Point Scales. *Field Methods* 24, 3 (2012), 310–327. https://doi.org/10.1177/1525822X12444061

[18] Nina Gerber, Benjamin Reinheimer, and Melanie Volkamer. 2018. Home Sweet Home? Investigating Users' Awareness of Smart Home Privacy Threats. In *Proceedings of An Interactive Workshop on the Human aspects of Smarthome Security and Privacy (WSSP)*. USENIX, Baltimore, MD, USA. https://doi.org/10.5445/IR/1000083578

[19] Timo Goeschl. 2019. Cold Case: The forensic economics of energy efficiency labels for domestic refrigeration appliances. *Energy Economics* 84 (2019), 104468.

[20] Roberto Hoyle, Luke Stark, Qatrunnada Ismail, David Crandall, Apu Kapadia, and Denise Anthony. 2020. Privacy Norms and Preferences for Photos Posted Online. *ACM Trans. Comput.-Hum. Interact.* 27, 4, Article 30 (aug 2020), 27 pages. https://doi.org/10.1145/3380960

[21] Haojian Jin, Boyuan Guo, Rituparna Roychoudhury, Yaxing Yao, Swarun Kumar, Yuvraj Agarwal, and Jason I. Hong. 2022. Exploring the Needs of Users for Supporting Privacy-Protective Behaviors in Smart Homes. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 449, 19 pages. https://doi.org/10.1145/3491102.3517602

[22] Nari Kim, Juntae Kim, Bomin Kim, and Young-Woo Park. 2021. The Trial of Posit in Shared Offices: Controlling Disclosure Levels of Schedule Data for Privacy by Changing the Placement of a Personal Interactive Calendar. In *Proceedings of the 2021 ACM Designing Interactive Systems Conference* (Virtual Event, USA) *(DIS '21)*. Association for Computing Machinery, New York, NY, USA, 149–159. https://doi.org/10.1145/3461778.3462073

[23] Spyros Kokolakis. 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security* 64 (2017), 122–134. https://doi.org/10.1016/j.cose.2015.07.002

[24] Hyosun Kwon, Joel E Fischer, Martin Flintham, and James Colley. 2018. The connected shower: Studying intimate data in everyday life. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 4 (2018), 1–22.

[25] Evan Lafontaine, Aafaq Sabir, and Anupam Das. 2021. Understanding People's Attitude and Concerns towards Adopting IoT Devices. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems (CHI'21)*. Association for Computing Machinery, New York, NY, USA, Article 307, 10 pages. https://doi.org/10.1145/3411763.3451633

[26] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, Are You Listening? Privacy Perceptions, Concerns and Privacy-Seeking Behaviors with Smart Speakers. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 102 (nov 2018), 31 pages. https://doi.org/10.1145/3274371

[27] Roxanne Leitão. 2019. In *Proceedings of the 2019 on Designing Interactive Systems Conference* (San Diego, CA, USA) *(DIS '19)*. Association for Computing Machinery, New York, NY, USA, 527–539. https://doi.org/10.1145/3322276.3322366

[28] Kun Liu and Evimaria Terzi. 2010. A Framework for Computing the Privacy Scores of Users in Online Social Networks. *ACM Trans. Knowl. Discov. Data* 5, 1, Article 6 (dec 2010), 30 pages. https://doi.org/10.1145/1870096.1870102

[29] Naresh K. Malhotra, Sung S. Kim, and James Agarwal. 2004. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research* 15, 4 (2004), 336–355. http://www.jstor.org/stable/23015787

[30] Nathan Malkin, Julia Bernd, Maritza Johnson, and Serge Egelman. 2018. "What Can't Data Be Used For?" Privacy Expectations about Smart TVs in the US. In *Proceedings of the 3rd European Workshop on Usable Security (EuroUSEC), London, UK.* https://doi.org/10.14722/eurousec.2018.23016

[31] Nathan Malkin, Joe Deatrick, Allen Tong, Primal Wijesekera, Serge Egelman, and David Wagner. 2019. Privacy attitudes of smart speaker users. *Proceedings on Privacy Enhancing Technologies* 2019, 4 (2019). https://doi.org/10.2478/popets-2019-0068

[32] Justin Matejka, Michael Glueck, Tovi Grossman, and George Fitzmaurice. 2016. The Effect of Visual Appearance on the Performance of Continuous Sliders and Visual Analogue Scales. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '16)*. Association for Computing Machinery, New York, NY, USA, 5421–5432. https://doi.org/10.1145/2858036.2858063

[33] Andrés Molina-Markham, Prashant Shenoy, Kevin Fu, Emmanuel Cecchet, and David Irwin. 2010. Private Memoirs of a Smart Meter. In *Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building* (Zurich, Switzerland) *(BuildSys '10)*. Association for Computing Machinery, New York, NY, USA, 61–66. https://doi.org/10.1145/1878431.1878446

[34] David H. Nguyen, Alfred Kobsa, and Gillian R. Hayes. 2008. An Empirical Investigation of Concerns of Everyday Tracking and Recording Technologies. In *Proceedings of the 10th International Conference on Ubiquitous Computing* (Seoul, Korea) *(UbiComp '08)*. Association for Computing Machinery, New York, NY, USA, 182–191. https://doi.org/10.1145/1409635.1409661

[35] Johannes Obermaier and Martin Hutle. 2016. Analyzing the Security and Privacy of Cloud-Based Video Surveillance Systems. In *Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security* (Xi'an, China) *(IoTPTS '16)*. Association for Computing Machinery, New York, NY, USA, 22–28. https://doi.org/10.1145/2899007.2899008

[36] Pascal Oser, Rens W. van der Heijden, Stefan Lüders, and Frank Kargl. 2022. Risk Prediction of IoT Devices Based on Vulnerability Analysis. *ACM Trans. Priv. Secur.* 25, 2, Article 14 (may 2022), 36 pages. https://doi.org/10.1145/3510360

[37] Charlie Parker, Sam Scott, and Alistair Geddes. 2019. Snowball sampling. *SAGE research methods foundations* (2019).

[38] Ulf-Dietrich Reips and Frederik Funke. 2008. Interval-level measurement with visual analogue scales in Internet-based research: VAS Generator. *Behavior Research Methods* 40, 3 (01 Aug 2008), 699–704. https://doi.org/10.3758/BRM.40.3.699

[39] Russell L. Rothman, Ryan Housam, Hilary Weiss, Dianne Davis, Rebecca Gregory, Tebeb Gebretsadik, Ayumi Shintani, and Tom A. Elasy. 2006. Patient Understanding of Food Labels: The Role of Literacy and Numeracy. *American Journal of Preventive Medicine* 31, 5 (2006), 391–398. https://doi.org/10.1016/j.amepre.2006.07.025

[40] Tanuja Singh and Mark E Hill. 2003. Consumer privacy and the Internet in Europe: a view from Germany. *Journal of consumer marketing* (2003).

[41] Christian Tiefenau, Maximilian Häring, Eva Gerlitz, and Emanuel von Zezschwitz. 2019. Making Privacy Graspable: Can we Nudge Users to use Privacy Enhancing Techniques? https://doi.org/10.48550/ARXIV.1911.07701

[42] Federico G Topolansky Barbe, Magdalena M Gonzalez-Triay, and Anna Hensel. 2013. Eco-labels in Germany. *Journal of customer behaviour* 12, 4 (2013), 341–359.

[43] Signe Waechter, Bernadette Sütterlin, and Michael Siegrist. 2015. The misleading effect of energy efficiency information on perceived energy friendliness of electric goods. *Journal of Cleaner Production* 93 (2015), 193–202. https://doi.org/10.1016/j.jclepro.2015.01.011

[44] Maximiliane Windl, Niels Henze, Albrecht Schmidt, and Sebastian S. Feger. 2022. Automating Contextual Privacy Policies: Design and Evaluation of a Production Tool for Digital Consumer Privacy Awareness. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 34, 18 pages. https://doi.org/10.1145/3491102.3517688

[45] Maximiliane Windl and Sven Mayer. 2022. The Skewed Privacy Concerns of Bystanders in Smart Environments. *Proc. ACM Hum.-Comput. Interact.* 6, MHCI, Article 184 (sep 2022), 21 pages. https://doi.org/10.1145/3546719

[46] Maximiliane Windl, Albrecht Schmidt, and Sebastian S. Feger. 2023. Investigating Tangible Privacy-Preserving Mechanisms for Future Smart Homes. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 70, 16 pages. https://doi.org/10.1145/3544548.3581167

[47] Peter Worthy, Ben Matthews, and Stephen Viller. 2016. Trust Me: Doubts and Concerns Living with the Internet of Things. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems* (Brisbane, QLD, Australia) *(DIS '16)*. Association for Computing Machinery, New York, NY, USA, 427–434. https://doi.org/10.1145/2901790.2901890

[48] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User Perceptions of Smart Home IoT Privacy. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 200 (nov 2018), 20 pages. https://doi.org/10.1145/3274469

# A INTERACTION SURVEY QUESTIONNAIRE

(1) IUIPC

(2) **Task 1:** Immerse yourself in the following situation: You want to buy a smart display for your home. On the device's box is a QR code that leads you to the following website. Please configure the device's connectivity and sensors according to your preferences. Configure the device and answer the questions from the perspective of a person wanting to purchase a smart display for their home.
[iFrame with interactive label embedded]
  (a) Did you configure the device from the perspective of a person who wants to purchase a smart display? (Sanity check)
  (b) Describe in at least one sentence why you configured the device this way. What were your key considerations? (Free text)
  (c) The website strongly supported me in making an informed decision. (Slider)
  (d) The features were most important to me when configuring the device. (Slider)
  (e) My data privacy was most important to me when configuring the device. (Slider)

(3) **Task 2:** Choose a device: Which of the following devices would you be most likely to buy? Please click on the image to view it in full size.
  (a) *Three images showing privacy labels for three different devices: One with a low privacy index and many features, one with a medium privacy index and a medium amount of features, and one with a high privacy index and low amount of features.* (Multiple choice)
  (b) Please describe in detail which factors influenced your purchase decisions. (Free text)

(4) **Task 3:** Please configure the device according to the following description: A user owns two Smart Beta displays. Please configure these devices according to the following description: The user wants both devices to be able to always react to voice commands. The user also wants to be able to do calls on both devices. However, only the device in the kitchen should allow video calls. The device in the bathroom should not allow access to the camera. Tip: When unsure about the different connectivity modes (i.e., online, local network, access point, and offline), you can hover over the small question mark icons to receive an explanation.
[iFrame with interactive label embedded]
  (a) What is the Privacy Index for the device placed in the kitchen? (Numeric entry field)
  (b) What is the Privacy Index for the device placed in the bathroom? (Numeric entry field)

(5) **Task 4:** Please configure the device according to the following description: The user's partner does not like the

fact that the devices can send data across the internet. However, the partner does like to use the *Advanced configuration* and *Limited remote access within home* features. Configure the label accordingly.
[iFrame with interactive label embedded]

(a) What is the Privacy Index of the device? (Numeric entry field)

# B APPLICABILITY SURVEY QUESTIONNAIRE

(1) IUIPC

(2) **Baseline Condition:** Immerse yourself in the following situation: You want to purchase [device name] for your home. The following is a reference to the official product page and allows you to get more information on the product if needed. Please carefully study the information and then answer the questions. You can revisit this product page anytime while answering the questions.
[iFrame with official product page embedded]
**Established Privacy Label Condition:** Immerse yourself in the following situation: You want to purchase [device name] for your home. Please carefully study the following privacy label for this device. Then, answer the questions. You can revisit this privacy label anytime while answering the questions.
[iFrame with established label embedded]
**Interactive Privacy Label Condition:** Immerse yourself in the following situation: You want to purchase [device name] for your home. Please carefully study the following privacy label for this device. The label is interactive and allows you to explore the various sensor settings and connectivity modes. You can revisit this privacy label anytime while answering the questions.
[iFrame with interactive label embedded]
We are interested in your perception of the different sensors of the [device name]. The following block of questions will be repeated for every sensor.

(a) Please list one single [device name] sensor. (Free text)

(b) Which of the following statements is true regarding the [entered sensor named]? (Single choice)

(i) The device allows me to disable the sensor.

(ii) The device does not allow me to disable the sensor.

(c) Please indicate your agreement with the following statement: I feel like I would most likely deactivate the [entered sensor name]. (Slider)

(d) Does the [device name] have more sensors? (Single choice - if yes, block repeated)

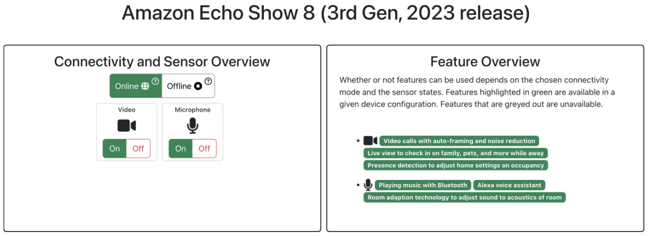
(3) **Final questions:** Please indicate your agreement regarding the following statements. (Slider)

(a) It is very important to me to learn which sensors smart home devices have.

(b) It is very important to me to learn whether I can deactivate the individual sensors of smart home devices.

(c) It is very important to me to learn about the privacy implications of the individual sensors of smart home devices.

(d) It was easy to find information about the types of sensors installed in smart home devices.


Amazon Echo Show 8 (3rd Gen, 2023 release)

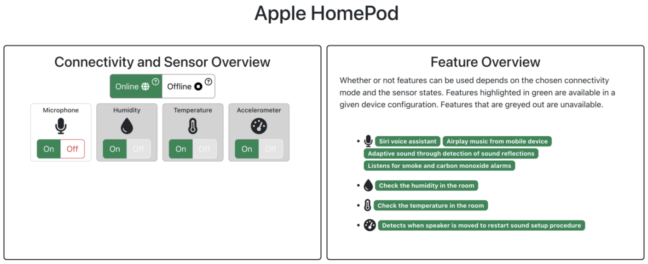
Connectivity and Sensor Overview

Feature Overview

Whether or not features can be used depends on the chosen connectivity mode and the sensor states. Features highlighted in green are available in a given device configuration. Features that are greyed out are unavailable.

- Video calls with auto-framing and noise reduction
  Live view to check in on family, pets, and more while away
  Presence detection to adjust home settings on occupancy
- Playing music with Bluetooth
  Alexa voice assistant
  Room adaption technology to adjust sound to acoustics of room

**Figure 8: The interactive privacy label we used in the survey for the Amazon Echo Show 8. The features and sensors were extracted from the manufacturer's official product pages.**


Apple HomePod

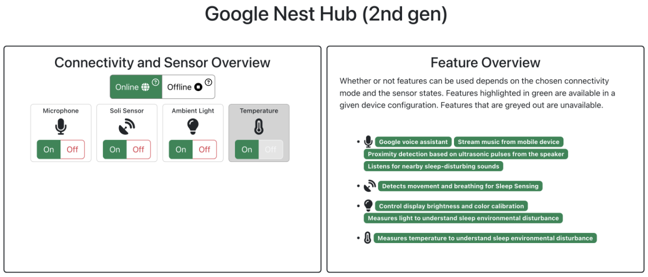
Connectivity and Sensor Overview

Feature Overview

Whether or not features can be used depends on the chosen connectivity mode and the sensor states. Features highlighted in green are available in a given device configuration. Features that are greyed out are unavailable.

- Siri voice assistant
  Airplay music from mobile device
  Adaptive sound through detection of sound reflections
  Listens for smoke and carbon monoxide alarms
- Check the humidity in the room
- Check the temperature in the room
- Detects when speaker is moved to restart sound setup procedure

**Figure 9: The interactive privacy label we used in the survey for the Apple HomePod. The features and sensors were extracted from the manufacturer's official product pages.**


Google Nest Hub (2nd gen)

Connectivity and Sensor Overview

Feature Overview

Whether or not features can be used depends on the chosen connectivity mode and the sensor states. Features highlighted in green are available in a given device configuration. Features that are greyed out are unavailable.

- Google voice assistant
  Stream music from mobile device
  Proximity detection based on ultrasonic pulses from the speaker
  Listens for nearby sleep-disturbing sounds
- Detects movement and breathing for Sleep Sensing
- Control display brightness and color calibration
  Measures light to understand sleep environmental disturbance
- Measures temperature to understand sleep environmental disturbance

**Figure 10: The interactive privacy label we used in the survey for the Google Nest Hub. The features and sensors were extracted from the manufacturer's official product pages.**

(e) It was easy to understand which sensors I could disable.

(f) I understand the consequences of enabling/disabling sensors on the device behavior.