

Smart Home Users’ Security and Privacy Perceptions and Actions Differ By Device Category: Results from a U.S. Survey

Julie M. Haney¹[0000–0002–6017–9693], Yasemin Acar²[0000–0001–7167–7383], Anna Li³, and Faith Haney⁴

¹ National Institute of Standards and Technology, Gaithersburg MD 20899, USA

`julie.haney@nist.gov`

² Paderborn University, 33098 Paderborn, Germany

`yasemin.acar@uni-paderborn.de`

³ Massachusetts Institute of Technology, Cambridge MA 02139, USA

`annawli@mit.edu`

⁴ University of Maryland, College Park MD 20742, USA `fhaney@umd.edu`

Abstract. There are few insights into how users’ perspectives on smart home security and privacy differ depending on device category. This may leave the smart home community at a disadvantage in knowing how to focus user education efforts to address device-specific misunderstandings or concerns. As a result, consumers may remain uninformed or lack motivation to protect some device categories, leaving devices and data vulnerable. Towards closing this gap, we conducted a between-subjects survey of 401 U.S. smart home users with devices in five categories: voice assistants, thermostats, security devices, sensors, and lighting. Participants found voice assistants to be most problematic and were most confident about security devices and thermostats. We also report novel results related to lack of trust of lighting device manufacturers and general comfort with sensor security and privacy. Our identification of differences across device categories can contribute to greater user empowerment through tailored smart home user education materials.

Keywords: Security · Smart home · Internet of things · Users.

1 Introduction

Internet of things (IoT) smart home research reveals that users may have inaccurate mental models of device security and privacy, exhibit lingering concerns even after adopting devices, struggle with a lack of transparency about data collection and use, and feel powerless to take action [22,53]. As a result, smart home devices and the data they collect may remain vulnerable to compromise.

Researchers suggest that user education may help counter these issues [53,63]. Device manufacturers play an important role in education, as reflected in IoT security baselines and guidance from government [3,17,42], industry [9,29], and standards [16] organizations. These baselines (minimum controls to sufficiently

safeguard a device against threats) require that manufacturers provide consumers with information about the presence, use, and implications of device security mechanisms and options. Additionally, several IoT product security labels are emerging to encourage manufacturers to build products to these minimum baselines [40,54,11]. Beyond the baseline requirements for manufacturers to provide user education, a labeling program includes its own education component to ensure users understand the purpose and risks addressed by the label and their own responsibility in protecting devices [42].

User education should address current user concerns, challenges, and misconceptions [34,42,62]. However, since IoT devices are diverse in functionality and data collection, users' perceptions and actions may differ depending on the type of device, i.e., device category [19,62]. For example, consumers may be concerned about leakage of voice assistant audio recordings but unconcerned about smart thermostat settings becoming public. Therefore, for user education to be effective, it needs to go beyond generic information that may not address these device-category nuances [23].

In our research, we focus on smart home devices (a subset of IoT), given their broad adoption and implications for private households [51]. Although most existing IoT baselines and labels focus on security, we recognize security and privacy are interconnected [41], so consider both in our work. Current smart home research that could inform the development of user education is typically device-agnostic or focused on a small subset of device categories, most commonly, voice assistants/smart speakers [46]. To systematically inform user education, we aim to extend prior research by understanding the differences in how users perceive and act on security and privacy across a range of popular device categories.

We conducted a survey of 401 demographically-diverse U.S. smart home users. The between-subjects survey was completed by participants answering questions about devices in five categories: voice assistants (e.g., Amazon Alexa, Google Home), thermostats (e.g., Google Nest, Ecobee thermostat), security devices (e.g., security cameras, door locks), sensors (e.g., smoke and water leak detectors), and lighting (e.g., light bulbs, lighting systems). We sought to answer the following research questions:

- RQ1:** How do users' perceptions about the security and privacy of their smart home devices differ across device categories?
- RQ2:** How do users' security and privacy actions and perceptions about taking action differ across device categories?

We found several device category distinctions, particularly for voice assistants, which participants believed to be less secure and privacy-protecting and more difficult to protect. Participants with security devices were more trusting of manufacturers and felt more capable protecting their devices. In contrast to prior literature [23], we found no evidence that lighting devices were devalued.

Our study makes several contributions. We extend prior research by providing new evidence that user security and privacy perceptions and actions differ across a broader range of device categories than has previously been investigated.

We further supply novel insights for smart home device categories (thermostats, sensors, lighting) that have rarely been intentionally explored from a user perspective, despite their popularity. These insights highlight users' challenges and potential misconceptions that may limit their motivation and ability to take meaningful action to protect their smart home devices and data. These results can inform manufacturers and label program administrators in the prioritization and development of smart home user education materials that address category-specific misconceptions, emphasize areas of particular concern and challenge to users, and empower users to take security and privacy actions.

2 Related Work

2.1 Smart Home Security and Privacy Perceptions and Actions

Users' smart home security concerns typically center on hacking to gain control of devices with the purpose of harassment or creating technical problems [24,62]. Conversely, risks affecting others outside the home, such as botnets, are not as important to users [63]. Privacy concerns are often associated with security failures, for example, data breaches. Users also express concern about their inability to control smart home data collection and use, with unwanted collection leading to surveillance, targeted advertisements, or inferences about household members [24,34,53,63]. Researchers found devices that collect sensitive audio or video data are generally perceived as less secure and privacy-protecting and, therefore, of more concern [15,23,53,62]. Devices for which a compromise could result in safety issues were likewise of more concern [24,26]. However, smart home adopters ultimately overcome their concerns, often because of manufacturer trust, willingness to accept risks in exchange for benefits, or confidence in their mitigation strategies [24,34,53]. Additionally, biases contribute to users' risk acceptance, for example, a fatalistic resignation that data are "already out there anyway," or optimism that they will not be targeted [24,34,53].

Some smart home users take actions to address concerns, for example, setting passwords, configuring device options, keeping devices out of private areas of the home, limiting data retention, and installing updates [24,34,53]. Users may take more action for devices with safety purposes or that collect sensitive audio and video data [30]. In contrast, they take fewer actions for simple-functionality devices that collect data perceived to be less sensitive, such as light bulbs and thermostats [15,14,23,30]. Many do not take substantive action for a variety of reasons, including limited understanding of device security and privacy or not being aware of device options [24,34,53]. For more empowerment, users' wish lists include greater control of data collection, easy-to-configure security/privacy options, and more information about risks and mitigations [24,30,60].

Our study extends these works by considering how device categories influence users' smart home security and privacy perceptions and actions. By sampling a diverse U.S. population, we uniquely quantify the magnitude of perceptions and challenges identified in prior qualitative studies with smaller, less-diverse samples (e.g., [53,61,62]). We also bring a broader focus than prior studies compar-

ing device categories, which addressed security/privacy information influence on purchase decisions [15,14], updates [19,23], and privacy-protective behaviors [30].

2.2 Labels

Researchers propose product labels to raise awareness of smart home security and privacy and inform purchase decisions [5,21,25]. Singapore [11] and Finland [40] have adopted IoT security labels, with other countries, such as the U.S. [54], to follow. An accompanying consumer education capability is considered essential in helping users understand how the label addresses product risks, addressing potential misconceptions, and describing users' role in device protection [42,43]. Since current user education guidance is generic, our discoveries can inform more meaningful communications unique to specific device categories.

3 Methodology

3.1 Study Design

We selected a survey format to allow for efficient sampling of a large number of users and leveraging prior qualitative work to inform survey development. While survey self-report data may be subject to selection or recall bias, perceptions are known to influence behavior [7], and it is important to understand areas of misconception or overconfidence so these can be addressed.

Between-Subjects Design. Our study was, in part, inspired by a prior within-subjects survey exploring device category differences for smart home updates [23]. We opted instead for a between-subjects design—in which participants answered questions for only one device category—to mitigate weaknesses of within-subjects surveys. While greater statistical power can be gained through a smaller number of participants in a within-subjects study, results are more likely to be impacted by potential demand effects (participants interpreting experimenter intentions based on the comparisons), range effects (responses potentially influenced by perceived range of presented items and a central tendency), and ordering effects (presentation of the compared items) [6,48]. Conversely, a between-subjects survey minimizes the transfer across conditions [4].

Topics. In this paper, we report survey results on the following topics related to our research questions and informed by the cited literature: perceptions about device security/privacy [23]; level of security/privacy concern [23]; reasons for lack of security/privacy concern or using devices despite concerns [24,22,53,62]; security/privacy actions taken by users [24,53,61]; perceived ability to secure devices and protect privacy [22,34]; and perceived barriers to taking security/privacy action [24,53,62]. For several topics, we asked paired security and privacy questions to account for potential differences. To distinguish security and privacy, we defined each term for participants.

Selection of Device Categories. The survey focused on five device categories. We selected these categories as a basis of comparison with related studies (e.g., [23]), since they are popular in the U.S. [44] [51], and because they represent diverse functionalities and data types that could impact users' security and privacy perceptions and actions. We describe each device category below.

Voice assistants (virtual assistants, smart speakers) carry out tasks via voice command. User concerns about these devices most often focus on protection of data, including the possibility of personal data (e.g., voice commands) being leaked [10,34,37].

Smart thermostats are connected devices that allow users to adjust and automate home temperature settings. Thermostats introduce risks since they collect and maintain information that could reveal household members' habits [55] and enact physical changes that can pose safety issues if hacked [49].

Smart security devices contribute to the physical security and safety of a home. Examples include security cameras, video doorbells, and door locks. Since these devices collect sensitive information and have safety implications, users are often most concerned about privacy risks (e.g., surveillance) [24,53] and hacking with the intent of disabling or controlling devices [24,53].

Smart sensors monitor and alert based on physical conditions within the home, often with a strong link to safety. Examples include water leak detectors, air quality monitors, and smoke detectors. Research on user perceptions of these devices is limited, with few public reports of attacks or vulnerabilities [33,50].

Smart lighting (e.g., light bulbs and lighting systems) allow users to automate lighting patterns and brightness for convenience or safety. While lighting has limited functionality, users express concern that operation could indicate a pattern of life [53]. Further, there are vulnerabilities that could result in information leakage or malware spread [36,39,18,57].

Review and Refinement. To confirm content and construct validity, we held three rounds of review to refine the survey instrument. An IoT security expert first checked for technical accuracy and alignment with research questions. In a second round, two survey experts evaluated language clarity and alignment of response options to questions. Finally, we held cognitive walk-throughs with two individuals representative of our target population for a final check of clarity.

3.2 Sampling Plan

Using GPower [20], we determined a minimum sample size of 305 for a Kruskal Wallis H Test with five independent groups (device categories) to achieve a power of 0.95, a medium effect size, and $\alpha = 0.05$. To meet and exceed this, we aimed for 400 participants (80 for each category).

We recruited participants using the Prodege opt-in consumer research panel. Participants had to be 18+ years old living in the U.S. and active users of smart home devices in at least one of the five categories. While our goal was not to

have a sample fully representative of the U.S. population, we wished to recruit participants from diverse demographic groups to survey a broad range of users. Thus, we developed optional targets to recruit a U.S. Census representative sample [58].

3.3 Data Collection and Participants

We fielded the survey for two weeks. Prospective participants completed a screening question about the smart home device categories they actively used. If they used a device in at least one category of interest, we randomly assigned them to complete the survey based on a selected category for which the participant quota (80) had not yet been met. If the participant indicated using only device categories with filled quotas, they were not invited to complete the survey. After a data quality check, 401 responses were included in the final dataset: 79 for voice assistants, 80 thermostats, 80 security devices, 80 sensors, and 82 lighting.

Table 1 shows participant demographics. Compared to all U.S. adults, our participants were younger, more racially diverse, and more educated, with 178 reporting as male and 218 as female. Additionally, over half (58%) were smart home device administrators (responsible for installation and troubleshooting), 39% were active users but not administrators, and 3% selected “Other” or no response for role.

Table 1. Participant Demographics (N = 401)

Demographic	Sub-category	n	%	Pop %
Age Range	18 - 34	150	37%	26%
	35 - 54	125	31%	31%
	55+	120	30%	43%
	No answer	6	<2%	-
Race	White	256	64%	81%
	Black	60	16%	10%
	Asian	39	10%	6%
	Pac. Islander	5	1%	<1%
	Am. Indian	11	3%	1%
	Multi-racial	16	4%	<2%
	No answer	14	3%	-
Ethnicity	Hispanic/Latino	99	25%	13%
	Not Hispanic	296	74%	87%
	No answer	6	<2%	-
Education Level	High school & below	126	31%	38%
	Some college & Associate’s	116	29%	27%
	Bachelor’s & above	152	38%	24%
	No answer	7	<2%	-

Percentages are rounded to the nearest whole number. Pop % (population %) is based on U.S. Census Bureau’s CPS Basic Monthly survey for adults [58].

3.4 Analysis

We calculated descriptive statistics to summarize response frequencies and inferential statistics at a significance level of $\alpha = 0.05$. We determined device category differences for ordinal responses (e.g., level of security concern) with Kruskal-Wallis H tests and post-hoc Dunn's tests for pairwise comparisons with a Holm-Bonferroni [1] correction to account for multiple comparisons (significant results reported with the z statistic). We used ANOVA and post-hoc pairwise comparisons with a Holm-Bonferroni correction to explore differences for continuous data (number of security and privacy actions), reported with t . To analyze device category differences for categorical responses (e.g., reasons for not taking action), we employed an initial Chi-square test of independence across all categories, then post-hoc Chi-square tests with Holm-Bonferroni corrections for pairwise comparisons. We report significant Chi-square results (one degree of freedom) with χ^2 .

When applicable, we also compared responses from related security and privacy questions using matched pair statistical tests. For ordinal data (e.g., comparing level of security concern to privacy concern), we used the Wilcoxon signed rank test, reported with the z -statistic. For categorical data (e.g., comparing reasons for not taking security action vs. privacy action), we used McNemar's test, reported with χ^2 .

For each significant result, we report the effect size. A large effect size may indicate that a finding has practical significance, while a small effect size may indicate limited practicality [52] (Table 2).

Table 2. Effect indices and size thresholds. Reported effect sizes are absolute values.

Index	Test	Small	Medium	Large
Independent groups				
Cohen's d (d) [8]	Mann-Whitney, ANOVA	0.20	0.50	0.80
Cramer's V (V) [32]	Chi square (1 deg freedom)	0.10	0.30	0.50
Matched data				
Effect size (r) [45]	Wilcoxon signed-rank test	0.10	0.30	0.50
Odds ratio (OR) [38]	McNemar's test	1.22 (0.538,0.82]	1.86 (0.333,0.538]	3.00 (∞ ,0.333]

3.5 Ethics

Our institutional review board approved the study. The first survey screen displayed information about the study purpose, procedure, data protection, and participant rights. Survey questions were optional and data were anonymous. Participants received a \$12.50 gift card (average completion time 13 minutes).

4 Results

4.1 RQ1: Device Security and Privacy Perceptions

Participants rated voice assistants as least secure and privacy protecting. To understand perceptions of device security and privacy, we asked participants to rate their agreement (5-point scale strongly disagree to strongly agree) with two statements: “I think that most of these smart home devices are secure” and “I think that most of these smart home devices protect my privacy” (Fig. 1). Participants most often agreed/strongly agreed that smart security devices were secure (80%) and privacy-protecting (70%), followed by sensors (70% security, 61% privacy). Voice assistants had the lowest agreement levels for both security (35%) and privacy (39%), which were significantly less than all other device categories (Table 3). Device security ratings were significantly higher than privacy ratings for the security device category ($z = 2.36, r = 0.26$).

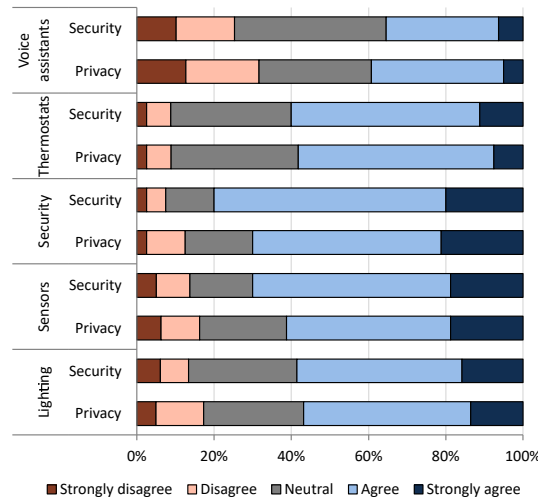


Fig. 1. Percentages of participants’ agreement ratings for the statements “I think that most of these smart home devices are secure” (Security) and “I think that most of these smart home devices protect my privacy” (Privacy).

The view that voice assistants are less secure and privacy-protecting did not translate into more concern. Participants rated their magnitude of device security and privacy concern (5-point scale from not at all to extremely concerned) (Fig. 2). Less than half of participants were moderately or extremely concerned about security, ranging from 42% and 41% for sensors and voice assistants, respectively, to 28% for thermostats and 31% for security devices. Concern ratings for privacy were similar, ranging from 42% for sensors and voice assistants to 31% for thermostats and security devices. There were no significant

Table 3. Significant device category differences for participants' ratings of agreement for the statements "I think that most of these smart home devices are secure" (Security) and "I think that most of these smart home devices protect my privacy" (Privacy).

Pairwise Comparison	Security (z, d)	Privacy (z, d)
Voice assistants - thermostats	-3.17, 0.56	-2.85, 0.55
Voice assistants - security	-5.51, 0.87	-4.55, 0.72
Voice assistants - sensors	-4.30, 0.61	-3.45, 0.52
Voice assistants - lighting	-3.15, 0.46	-2.74, 0.45

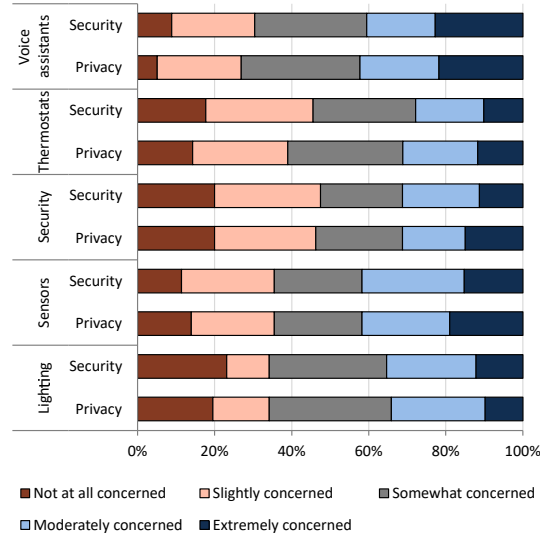


Fig. 2. Percentages of participants' ratings of level of smart home security and privacy concern per device category.

differences across categories. Participant ratings of security concern were significantly lower than ratings of privacy concern for the thermostat category ($z = -2.52$, $r = 0.39$).

Participants had varying beliefs contributing to their lack of concern, particularly for voice assistants, lighting, and thermostats. Participants selected reasons why they have little or no security or privacy concern or continue to use their devices even if concerned (Fig. 3). Each option was selected by fewer than 40%. "Benefits outweigh risks" was the most frequent response (38%), followed by "Data/devices aren't interesting enough to target" (31%) and "Chances of device being hacked are low" (31%). Less than 15% indicated an understanding of data collection/use or control over their data as reasons.

We found significant differences among device categories for three response options. Thermostat participants selected "Chances of device being hacked are low" significantly more often as compared to those with voice assistants ($\chi^2 =$

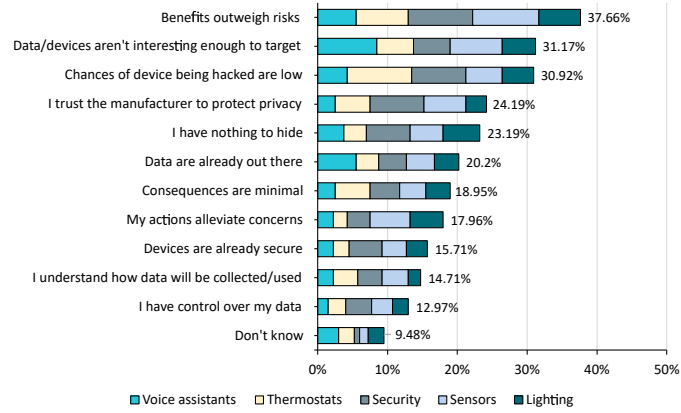


Fig. 3. Percentages of participants selecting reasons for not being concerned about smart home security/privacy or still using the devices despite being concerned.

10.84, $V = 0.26$) and lighting ($\chi^2 = 10.66$, $V = 0.26$). Thermostat participants also selected “My actions alleviate concerns” less often than those with sensors ($\chi^2 = 9.00$, $V = 0.24$). Finally, security device participants more often selected “I trust the manufacturer to protect my privacy” compared to those with voice assistants ($\chi^2 = 14.14$, $V = 0.30$) and lighting ($\chi^2 = 12.08$, $V = 0.27$).

4.2 RQ2: Security and Privacy Actions

Security and privacy actions were often simplistic, with more actions for security devices. Participants selected the actions they took to secure and protect the privacy of their devices (Fig. 4). Because some smart home device mitigations address both security and privacy concerns (e.g., setting a password) [24], we combined possible security and privacy device actions into a single question. No actions were selected by a majority. The most-selected action was setting a password/PIN on the device or app (49%). A third indicated they limit the amount of information entered in the device app. Slightly fewer said they use two-factor authentication. Almost 12% indicated they do not take any actions. Two participants selecting “Other” said they disconnect their devices.

We found several significant differences across device categories (Table 4). Participants more often selected setting a password/PIN for security devices as compared to voice assistants and lighting devices. Not placing the device in a sensitive or private area was selected less often for thermostats as compared to voice assistants and security devices. Participants said they were careful what they say or do near the device less often for thermostats than for any other device category. Finally, setting up or changing security/privacy settings for voice assistants was selected less often as compared to all other categories.

Participants took an average of 2.29 actions. Twenty-one percent took one action, 20% each took two or three actions, and 21% took four or more actions

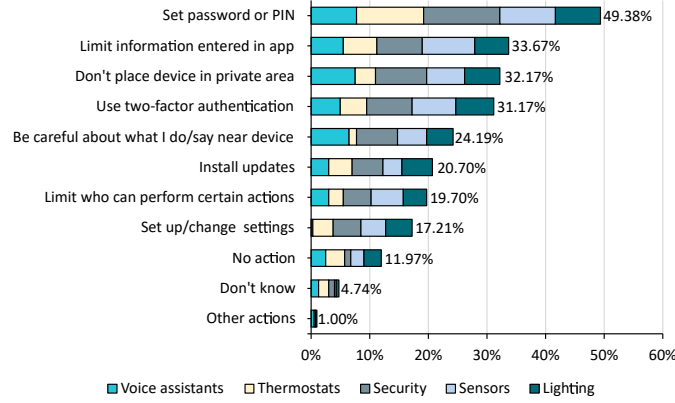


Fig. 4. Percentage of participants selecting security/privacy actions per device category.

(Fig. 5). Participants with security devices took significantly more actions as compared to those with voice assistants ($t = 3.46$, $d = 0.54$), thermostats ($t = 3.96$, $d = 0.60$), and lighting ($t = 1.27$, $d = 0.41$).

Table 4. Significant device category differences for security and privacy actions.

Action	Pairwise Comparison	χ^2 , V
Set password or PIN	security – voice assistants	10.57, 0.36
	security - lighting	11.99, 0.27
Don't place device in private area	thermostats – voice assistants	8.33, 0.23
	thermostats - security	12.97, 0.28
Be careful what I say/do near device	thermostats – voice assistants	18.00, 0.34
	thermostats – security	20.20, 0.36
	thermostats – sensors	10.67, 0.26
	thermostats – lighting	8.19, 0.22
Set up/change settings	voice assistants – thermostats	12.26, 0.28
	voice assistants – security	18.27, 0.34
	voice assistants – sensors	15.81, 0.32
	voice assistants – lighting	16.54, 0.32

Participants felt least able to protect their voice assistants. We asked participants to rate their agreement with the statements “I feel able to protect my smart home device’s security” and “I feel able to protect my privacy when using my smart home device” (Fig. 6). Over half agreed/strongly agreed with both statements for all categories except voice assistants (37% for security and privacy). For security, voice assistant participants had significantly lower agreements than security devices ($z = -3.21$, $d = 0.51$). For privacy, these same voice assistant participants had significantly lower agreement levels than all other categories: thermostats ($z = -2.83$, $d = 0.49$), security devices ($z = -3.51$, $d = 0.57$),

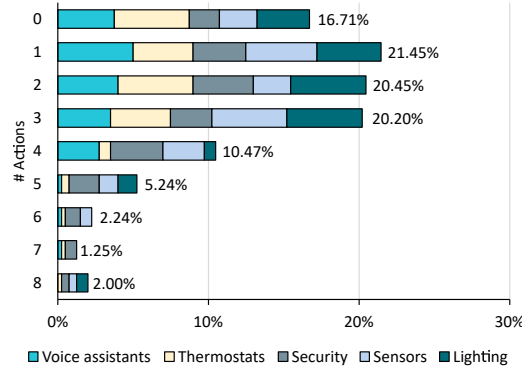


Fig. 5. Percentages of participants selecting 0 - 8 security/privacy actions per device category.

sensors ($z = -4.04$, $d = 0.62$), lighting ($z = -3.51$, $d = 0.56$). For the sensors category, participants’ agreement ratings for security ability were significantly lower than their ability to protect privacy ($z = -2.71$, $r = 0.30$).

Participants expressed varied obstacles to taking action, with thermostat respondents more satisfied with their actions and options. We asked participants what keeps them from taking action or more action than they already take to ease their security concerns, then what keeps them from taking action to ease their privacy concerns (Fig. 7). Less than 30% selected each option. The most common response for both security and privacy was “Nothing – I have taken action and am satisfied,” followed by “I do not understand smart home security/privacy enough to take action.” In addition, for privacy, 20% indicated that there are were not enough options for configuring preferences. For the lighting category, this option was selected significantly more for privacy barriers as compared to security ($\chi^2 = 5.00$, $OR = 0.333$). For both security and privacy, 9% said that nothing prevents them because they are not concerned.

We found one significant category difference for security obstacles: voice assistant participants indicated they had taken action and were satisfied less often compared to thermostat participants ($\chi^2 = 18.94$, $V = 0.35$). For privacy, participants less often indicated that there are no options for thermostats as compared to lighting ($\chi^2 = 8.57$, $V = 0.23$). Thermostat participants more often selected the “Nothing - taken action and satisfied” option as compared to those with voice assistants ($\chi^2 = 22.90$, $V = 0.38$), security devices ($\chi^2 = 10.99$, $V = 0.26$), and lighting ($\chi^2 = 9.41$, $V = 0.24$). Additionally, participants selected this same option significantly more for sensors than voice assistants ($\chi^2 = 9.90$, $V = 0.25$).

5 Discussion

In this section, we situate our results within the literature, address study limitations, and offer practical suggestions to inform education materials.

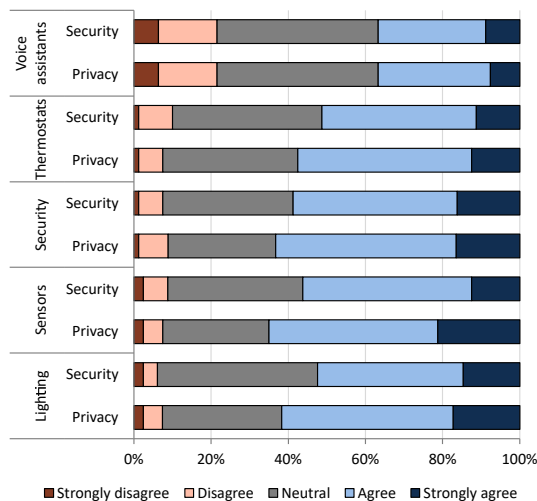


Fig. 6. Percentages of participants' ratings of agreement with the statements "I feel able to protect my smart home device's security" (Security) and "I feel able to protect my privacy when using my smart home device" (Privacy) per device category.

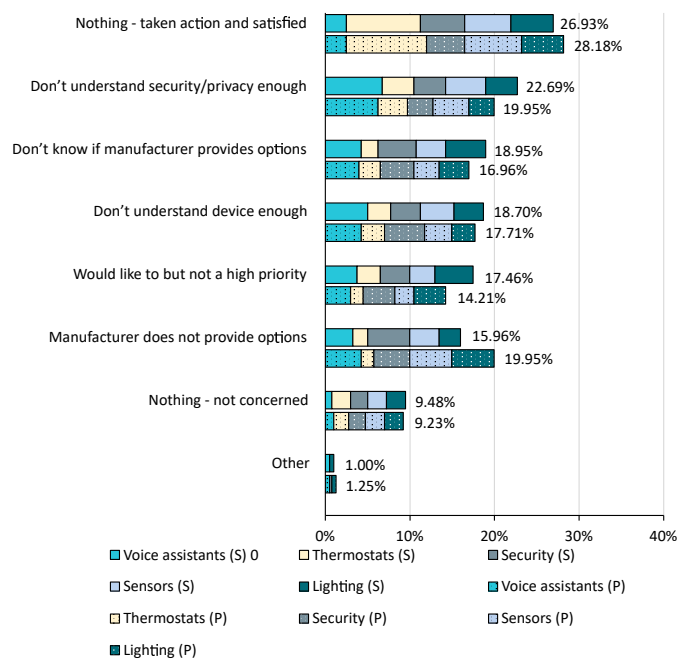


Fig. 7. Percentages of participants selecting obstacles to taking actions or taking more actions than they already have per device category. Security obstacles are presented first for each pair in solid colors and indicated with (S) in the legend. Privacy options have a dotted pattern and are indicated with (P).

5.1 Device Category Insights

Participants have a greater unease and lack of agency for voice assistants compared to other device categories. Results confirm other studies identifying negative perceptions about voice assistants, for example, doubt about data protection/use or lack of awareness of security/privacy options [14,34,37]. As adopters of voice assistants, our participants obviously overcame concerns, most commonly because they believe their data and device are not interesting enough to target and that benefits outweigh risks (Fig. 3). These beliefs may also explain why lower ratings of device security/privacy did not translate into greater concern; participants’ *intuitive concern* (ratings of device security/privacy) may differ from *considered concern*, which emerges after weighing risks and benefits and believing the likelihood of compromise is low [47].

Since participants with thermostats believe the chances of device hacking are low, they may not be inclined to take protective actions or may be satisfied with what they have already done. This is in line with prior work finding that few users have accurate mental models about thermostat privacy threats [30]. Additionally, the observation that participants are less likely to take actions related to device location is expected since thermostat placement is usually not within the control of users.

Participants are more actively involved in protecting their security devices. We note a divergence from prior work [23]; despite the collection of audio/video data, our participants viewed smart security devices as more secure and privacy-respecting than voice assistants, perhaps due to participants’ reported manufacturer trust (also identified in [26]). It may also be the case that participants assume devices with *physical* security purposes are similarly *cyber-secure* [56]. Interestingly, participants took active responsibility for protecting their security devices, perhaps motivated by the sensitivity of the data, safety implications should the devices fail, or feeling confident to act due to their awareness of configurable options (e.g., options that limit data retention) [26,30,53].

Participants generally believe sensors to be secure and privacy protecting (also found in [23]). As compared to other device categories, participants with sensors were also more satisfied with their security/privacy actions. Privacy findings are expected due to the less-sensitive data collected by these devices. However, we are surprised there was not more security concern due to potential safety implications (e.g., losing smoke detection) should the devices be hacked.

We provide novel insights about lighting perceptions. Our findings identify previously-unidentified distrust of smart lighting manufacturers, belief that the chance of hacking is perhaps higher than for other categories, and a more-frequent perception that there are not enough privacy options. These may indicate a growing recognition among users of how even simple devices can pose threats to the home network. Conversely, prior studies discovered a minimization of security and privacy risks to smart lighting [14,23,30].

5.2 Limitations and Future Work

Study results may not be generalizable. U.S. users may not have the same perceptions as those living elsewhere [12]. We also cannot generalize to other device categories. Future work could explore other populations and devices.

It is unclear which survey design most appropriately measures user perceptions in a natural setting. Our between-subjects survey results diverged from responses to identical questions (related to device security/privacy and security/privacy concern) in a within-subjects survey, for example that security devices were viewed as significantly less secure/private and lighting was of less concern [23]. We purposely selected our survey design to alleviate potential range and order effects present in the prior survey, as we asked participants to rate one device category in isolation as opposed to rating each category relative to others [6]. However, it is unclear as to which surveying method more accurately represents how users actually evaluate their smart home devices. It is possible that users do not consider comparisons between different device categories when purchasing a new device, in which case our between-subjects design may be more appropriate [6]. Conversely, users might engage in relative evaluation when they have multiple, interacting devices in their homes, in which case a within-subjects design could be advantageous. This more targeted exploration has implications for label user education programs, but is left for future research.

Users may conflate security and privacy. Although we defined both terms for participants, existing mental models might conflate these concepts, a common observation in prior research [24,31,62]. We did find a few significant differences between security and privacy response pairs, but with no device category patterns. We note that, while the distinction may be important for security, privacy, and legal experts [27], it may not be needed for most. Further, since this conflation could occur in real-world scenarios in which consumers are interpreting security/privacy labels or other information, we see a need for user education to progress beyond current confines of security towards addressing privacy needs and concerns prevalent among users (e.g., as recommended in [5,14]).

5.3 Practical Implications

Emphasize that all types of devices may be at risk. Our results may imply that, for some device categories (e.g., thermostats), users have a false sense of security and privacy, believing that these devices require less intervention or vigilance on the part of users or are less likely to be compromised. Such devices may not have clear safety applications, perform simple functions, or collect data considered to be less sensitive, all factors attributed to differences in device category perceptions in prior work [19,15,23]. However, these device data may still be used to infer household pattern of life [2,28] or be used as jumping off points for exploiting other, more valuable assets on the network [59]. Therefore, the reduction of devices into “sensitive” and “non-sensitive” may demonstrate a lack of understanding that could put users at risk [62].

Because security and privacy preferences and concerns can be contextual and complex [13,35], to overcome these potential misconceptions, manufacturers could tailor product-specific materials to discuss the likelihood and severity of risks as applicable to category-specific characteristics, such as functionality, exposure, sensitivity of collected data, and safety implications. They could additionally communicate that compromise of often-undervalued devices with simple functionality (like sensors or thermostats) might lead to compromise of other, higher-value devices on the home network. Moreover, since labels are meant to facilitate assurance in smart products, care should be taken to ensure users do not lose trust in the technology or confidence in their own ability to protect their devices, as our survey suggests is the case with voice assistants. Thus, manufacturers and label administrators should be honest about risks but also clearly state how security and privacy mechanisms help reduce risk.

Communicate what is expected of users and empower them to act.

While labels and their underlying baseline criteria strive to promote development of secure products, security privacy are not the sole responsibility of manufacturers. Therefore, user education recommendations call out the need to communicate expectations about consumers’ role in device protection [42]. To be successful in this role, users need to be empowered to take action, which may be more daunting for certain device categories, such as voice assistants, which may not have relevant options for users to configure [34]. Manufacturers can provide information and instructions on user-configurable security and privacy options available for their products, the implications and efficacy of user configuration choices, and home network-based mitigations to provide layered defenses (as also recommended in [24,53,61,62]). This information should be tied to category-specific risks and consequences in order to motivate users to act and overcome misconceptions about certain types of devices, as discussed above.

Utilize insights on user perceptions to prioritize the development of label profiles.

The minimum baselines products must meet to obtain product labels may require tailored, device category-specific implementations to address differences in functionality and technological constraints. This will be the case with recently-announced U.S. government plans for the U.S. Cyber Trust Mark labeling program for smart devices [54], in which the community (e.g., manufacturers, government) will develop multiple profiles tailored to IoT product categories [42]. Since the implementation of the U.S. label program likely will be incremental (one device category at a time), prioritizing the development of a label profile for the device categories identified as more problematic or less understood in our survey (e.g., voice assistants) may be advantageous in providing immediate impact and value to consumers. User education about the security and privacy features included in the products may help assuage the discomfort that some users harbor even after adopting those devices, as evidenced by the non-trivial number of participants who expressed moderate or extreme concern despite being active users of the devices (also found in [22,53,61,62]).

Disclaimer

Certain commercial companies or products are identified to foster understanding, not to imply recommendation or endorsement by the National Institute of Standards and Technology, nor to imply that these are necessarily the best available for the purpose.

References

1. Abdi, H.: Holm's sequential bonferroni procedure. *Encyclopedia of research design* **1**(8), 1–8 (2010)
2. Apthorpe, N., Reisman, D., Feamster, N.: A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic. In: arXiv preprint arXiv:1705.06805 (2017)
3. Behavioural Economics Team of the Australian Government: Stay smart: Helping consumers choose cyber secure smart devices. <https://behaviouraleconomics.pmc.gov.au/sites/default/files/projects/beta-report-cyber-security-labels.pdf> (2022)
4. Budiu, R.: Between-subjects vs. within-subjects study design. <https://www.nngroup.com/articles/between-within-subjects/> (May 2018)
5. Carnegie Mellon University: IoT security and privacy label. <https://iotsecurityprivacy.org/> (2023)
6. Charness, G., Gneezy, U., Kuhn, M.A.: Experimental methods: Between-subject and within-subject design. *Journal of Economic Behavior & Organization* **81**(1), 1–8 (2012)
7. Chen, Y., Zahedi, F.M.: Individuals' internet security perceptions and behaviors. *MIS Quarterly* **40**(1), 205–222 (2016)
8. Cohen, J.: A power primer. *Psychological Bulletin [PscyARTICLES]* (1) (July 1992)
9. Council to Secure the Digital Economy: The C2 consensus on IoT security baseline capabilities. <https://securingdigitaleconomy.org/projects/c2-consensus/> (2019)
10. Cowan, B.R., Pantidi, N., Coyle, D., Morrissey, K., Clarke, P., Al-Shehri, S., Earley, D., Bandeira, N.: "what can i help you with?" infrequent users' experiences of intelligent personal assistants. In: *Proceedings of the 19th International Conference on Human-Computer Interaction with Mobile Devices and Services*. pp. 1–12 (2017)
11. Cyber Security Agency of Singapore: Cybersecurity labelling scheme. <https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme> (2023)
12. Dogruel, L., Joeckel, S.: Risk perception and privacy regulation preferences from a cross-cultural perspective: A qualitative study among German and US smartphone users. *International Journal of Communication* **13**, 20 (2019)
13. Emami-Naeini, P., Bhagavatula, S., Habib, H., Degeling, M., Bauer, L., Cranor, L.F., Sadeh, N.: Privacy expectations and preferences in an IoT world. In: *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. pp. 399–412 (2017)
14. Emami-Naeini, P., Dheenadhayalan, J., Agarwal, Y., Cranor, L.F.: Which privacy and security attributes most impact consumers' risk perception and willingness to purchase IoT devices? In: *2021 IEEE Symposium on Security and Privacy (SP)*. pp. 1937–1954 (2021)

15. Emami-Naeini, P., Dixon, H., Agarwal, Y., Cranor, L.F.: Exploring how privacy and security factor into IoT device purchase behavior. In: CHI Conference on Human Factors in Computing Systems. ACM (2019)
16. ETSI Technical Committee Cyber Security: ETSI EN 303 645 V2.1.1 cyber security for consumer internet of things: Baseline requirements. https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf (2020)
17. European Union Agency for Cybersecurity: Good practices for security of IoT - Secure software development lifecycle. <https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1> (2019)
18. Fagan, M., Yang, M., Tan, A., Randolph, L., Scarfone, K.: Draft NISTIR 8267 Security review of consumer home Internet of Things (IoT) products. <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8267-draft.pdf> (2019)
19. Fassel, M., Neumayr, M., Schedler, O., Krombholz, K.: Transferring update behavior from smartphones to smart consumer devices. In: 27th European Symposium on Research in Computer Security (ESORICS) (2021)
20. Faul, F., Erdfelder, E., Buchner, A., Lang, A.G.: Statistical power analyses using g^* power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods* **41**(4), 1149–1160 (2009)
21. Gopavaram, S., Dev, J., Das, S., Camp, L.J.: Iot marketplace: Willingness-to-pay vs. willingness-to-accept. In: Proceedings of the 20th Annual Workshop on the Economics of Information Security (WEIS 2021) (2021)
22. Haney, J., Acar, Y., Furman, S.: “It’s the company, the government, you and I”: User perceptions of responsibility for smart home privacy and security. In: 30th USENIX Security Symposium. pp. 411–438 (2021)
23. Haney, J.M., Furman, S.M.: User perceptions and experiences with smart home updates. In: Proceedings of the 2023 IEEE Symposium on Security & Privacy (2023)
24. Haney, J.M., Furman, S.M., Acar, Y.: Smart home security and privacy mitigations: Consumer perceptions, practices, and challenges. In: International Conference on Human-Computer Interaction. pp. 393–411 (2020)
25. Harris Interactive: Consumer internet of things security labelling survey research findings. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/798543/Harris_Interactive_Consumer_IoT_Security_-Labelling_Survey_Report.pdf (2019)
26. Hazazi, H., Shehab, M.: Exploring the usability, security, and privacy of smart locks from the perspective of the end user. In: Proceedings of the 19th Symposium on Usable Privacy and Security (2023)
27. Heckman, M.R.: United States Cybersecurity Magazine (2017)
28. Hill, K., Mattu, S.: The house that spied on me. <https://gizmodo.com/the-house-that-spied-on-me-1822429852> (2018)
29. IoT Security Foundation: Iot security assurance framework. <https://iotsecurityfoundation.org/wp-content/uploads/2021/11/IoTSF-IoT-Security-Assurance-Framework-Release-3.0-Nov-2021-1.pdf> (2021)
30. Jin, H., Guo, B., Roychoudhury, R., Yao, Y., Kumar, S., Agarwal, Y., Hong, J.I.: Exploring the needs of users for supporting privacy-protective behaviors in smart homes. pp. 1–19 (2022)
31. Kang, R., Dabbish, L., Fruchter, N., Kiesler, S.: “my data just goes everywhere:” user mental models of the internet and implications for privacy and security. In: Eleventh Symposium on Usable Privacy and Security (SOUPS 2015) (2015)

32. Kim, H.Y.: Statistical notes for clinical researchers: Chi-squared test and fisher's exact test. *Restorative dentistry & endodontics* **42**(2), 152–155 (2017)
33. Kovacs, E.: Vulnerabilities allow hackers to access Honeywell fire alarm systems. <https://www.securityweek.com/vulnerabilities-allow-hackers-access-honeywell-fire-alarm-systems/> (Feb 2020)
34. Lau, J., Zimmerman, B., Schaub, F.: Alexa, are you listening?: Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. In: *ACM on Human-Computer Interaction*. ACM (2018)
35. Lutz, C., Newlands, G.: Privacy and smart speakers: A multi-dimensional approach. *The Information Society* **37**(3), 147–162 (2021)
36. Maiti, A., Jadliwala, M.: Light ears: Information leakage via smart lights. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* **3**(3), 1–27 (2019)
37. Malkin, N., Deatrck, J., Tong, A., Wijesekera, P., Egelman, S., Wagner, D.: Privacy attitudes of smart speaker users. *Privacy Enhancing Technologies* **2019**(4), 250–271 (2019)
38. Mangiafico, S.S.: Summary and analysis of extension program evaluation in r, version 1.20.05. <https://rcompanion.org/handbook/> (2023)
39. Morgner, P., Mattejat, S., Benenson, Z., Müller, C., Armknecht, F.: Insecure to the touch: Attacking ZigBee 3.0 via touchlink commissioning. In: *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. pp. 230–240 (2017)
40. National Cyber Security Centre Finland: Cybersecurity label. <https://tietoturvamerkki.fi/en/cybersecurity-label> (2023)
41. National Institute of Standards and Technology: NIST privacy framework: A tool for improving privacy through enterprise risk management, version 1.0. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf> (2020)
42. National Institute of Standards and Technology: Recommended criteria for cybersecurity labeling for consumer internet of things (IoT) products. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf> (Feb 2022)
43. National Institute of Standards and Technology: Report for the assistant to the president for national security affairs (APNSA) on cybersecurity labeling for consumers: internet of things (IoT) devices and software. <https://www.nist.gov/document/report-assistant-president-national-security-affairs-apnsa-cybersecurity-labeling-consumers> (May 2022)
44. NPD Group: Half of U.S. consumers own at least one smart home device. <https://www.npd.com/news/press-releases/2021/half-of-u-s-consumers-own-at-least-one-smart-home-device-reports-npd/> (2021)
45. Pallant, J.: *Survival manual: A step by step guide to data analysis using SPSS*. 4 edn. (2011)
46. Pattnaik, N., Li, S., Nurse, J.R.: A survey of user perspectives on security and privacy in a home networking environment. *ACM Computing Surveys* **55**(9), 180 (2023)
47. Phelan, C., Lampe, C., Resnick, P.: It's creepy, but it doesn't bother me. In: *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. pp. 5240–5251 (2016)
48. Poulton, E.: Unwanted range effects from using within-subject experimental designs. *Psychological Bulletin* **80**(2), 113–121 (1973)
49. Sears, A.: "felt so violated:" milwaukee couple warns hackers are outsmarting smart homes. <https://www.fox6now.com/news/felt-so-violated-milwaukee-couple-warns-hackers-are-outsmarting-smart-homes> (Sep 2019)

50. Sivaraman, V., Gharakheili, H.H., Fernandes, C., Clark, N., Karlychuk, T.: Smart IoT devices in the home: Security and privacy implications. *IEEE Technology and Society Magazine* **37**(2), 71–79 (2018)
51. Statista: Smart home device household penetration in the United States in 2019 and 2021. <https://www.statista.com/statistics/1247351/smart-home-device-us-household-penetration/> (2021)
52. Sullivan, G.M., Feinn, R.: Using effect size—or why the p value is not enough. *Journal of Graduate Medical Education* **4**(3), 279–282 (2012)
53. Tabassum, M., Kosiński, T., Lipford, H.R.: "I don't own the data": End user perceptions of smart home device data practices and risks. In: 15th Symposium on Usable Privacy and Security (2019)
54. The White House: Biden-harris administration announces cybersecurity labeling program for smart devices to protect american consumers. <https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/18/biden-harris-administration-announces-cybersecurity-labeling-program-for-smart-devices-to-protect-american-consumers/> (2023)
55. Thompson, D.: Is your smart thermostat a cybersecurity risk? <https://www.sciencetimes.com/articles/36048/20220210/is-your-smart-thermostat-a-cybersecurity-risk.htm> (Feb 2022)
56. Thompson, J.D., Herman, G.L., Scheponik, T., Oliva, L., Sherman, A., Golaszewski, E., Phatak, D., Patsourakos, K.: Student misconceptions about cybersecurity concepts: Analysis of think-aloud interviews. *Journal of Cybersecurity Education, Research and Practice* **2018**(1), 5 (2018)
57. Trend Micro: Researchers use smart light bulbs to infiltrate networks. <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/researchers-use-smart-light-bulbs-to-infiltrate-networks> (Feb 2020)
58. United States Census Bureau: Basic monthly cps. <https://www.census.gov/data/datasets/time-series/demo/cps/cps-basic.html> (2023)
59. Wei, W.: Casino gets hacked through its internet-connected fish tank thermometer. <https://thehackernews.com/2018/04/iot-hacking-thermometer.html> (Apr 2018)
60. Yao, Y., Basdeo, J.R., Kaushik, S., Wang, Y.: Defending my castle: A co-design study of privacy mechanisms for smart homes. In: CHI Conference on Human Factors in Computing Systems. pp. 1–12. ACM (2019)
61. Zeng, E., Mare, S., Roesner, F.: End user security and privacy concerns with smart homes. In: 13th Symposium on Usable Privacy and Security (2017)
62. Zheng, S., Apthorpe, N., Chetty, M., Feamster, N.: User perceptions of smart home IoT privacy. *ACM on Human-Computer Interaction* **2**(CSCW) (2018)
63. Zimmermann, V., Gerber, P., Marky, K., Bóck, L., Kirchbuchner, F.: Assessing users' privacy and security concerns of smart home technologies. *i-com* **18**(3), 197–216 (2019)