NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Special Publication (SP) 1343

Survey on Smart Home Users' Security and Privacy Perceptions and Actions: A Device Category Perspective

Julie Haney
Yasemin Acar
Anna Li
Faith Haney

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1343

NIST Special Publication (SP) 1343

Survey on Smart Home Users' Security and Privacy Perceptions and Actions: A Device Category Perspective

Julie Haney
Information Technology Laboratory, NIST

Yasemin Acar
Paderborn University

Anna Li
Massachusetts Institute of Technology

Faith Haney
University of Maryland

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1343

DECEMBER 2025

U.S. Department of Commerce
Howard Lutnick, Secretary

National Institute of Standards and Technology
Craig Burkhardt, Acting Under Secretary of Commerce for Standards and Technology and Acting NIST Director

Disclaimer

Certain commercial companies or products are identified in this report to foster understanding and provide details on the research. These inclusions do not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that these are necessarily the best available for the purpose.

NIST Technical Series Policies

Publication History

Approved by the NIST Editorial Review Board on: 2025-12-14

How to cite this NIST Technical Series Publication

Haney J., Acar, Y., Li, A., Haney, F. (2025)
Survey on Smart Home Users' Security and Privacy Perceptions and Actions: A Device Category Perspective
National Institute of Standards and Technology
Gaithersburg, MD
NIST Special Publication (SP) 1343.

https://doi.org/10.6028/NIST.SP.1343

NIST Author ORCID iDs

Julie Haney: 0000-0002-6017-9693

Contact Information

human-cybersec@nist.gov

ABSTRACT

Although smart home adoption in the United States (U.S.) is growing, smart home users may harbor security and privacy concerns or uncertainty about how to best protect their devices and the data those collect. Further, there have been 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 survey of 401 U.S. smart home users with devices in five categories: lighting, security devices, sensors, thermostats, and voice assistants. Participants viewed voice assistants as most problematic and were most confident about security devices and thermostats. We also report novel results related to perceptions of smart home security and privacy responsibility and users' thoughts on device categories seldom explored in research. Our identification of differences across device categories can contribute to greater user empowerment through tailored smart home user education materials.

KEYWORDS

smart home, internet of things, cybersecurity, privacy, human-centered cybersecurity, human factors

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Despite the growth of smart home adoption in the United States (U.S.), smart home users may harbor security and privacy concerns or uncertainty about how to best protect their devices and the data those devices collect. Further, there have been few insights into how users' perspectives on smart home security and privacy differ depending on device category (type) since devices may have varying sophistication levels of functionality, collect different types of data, and evoke different concerns. This lack of understanding 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 survey of 401 U.S. smart home users with devices in at least one of five categories: lighting, security devices (e.g., video doorbells, cameras, smart locks), sensors (e.g., water leak and smoke detectors), thermostats, and voice assistants (i.e., smart speakers, virtual assistants). We asked participants about their smart home security and privacy perceptions, the security and privacy actions they took, to whom they assign responsibility of smart home security and privacy, and their sources of smart home security and privacy information. We identified overall trends across all device types as well as category-specific trends.

The identification of differences across devices can inform smart home device manufacturers and security label programs (like the U.S. Cyber Trust Mark [FCC 2024]) to go beyond generic guidance by tailoring education materials to address the specific risks, security and privacy features, and expected user protective actions for individual device categories.

Findings

The following provides a high-level overview of study results.

Security and privacy perceptions:

- **Participants rated voice assistants as least secure and privacy protecting.** In contrast, well over half of participants believed that devices in other categories were secure and privacy-protecting.
- **Participants generally believed they understood the security and privacy risks of their smart home devices.** Over half of participants said that they understood the risks of their devices, with the most understanding for smart security devices and least for voice assistants.
- **A majority of participants were concerned about the security and privacy of their devices.** Between just over half and almost three-fourths of participants were at least somewhat concerned. Statistically speaking, there were no significant differences among device categories.

- **Participants had varying beliefs about security and privacy which, in part, could explain their levels of concern.** The top four reasons why they were not concerned or continued to use their devices despite being concerned were: benefits outweigh risks; data/devices are not interesting enough to target; chances of devices being hacked are low; and trust in the manufacturer to protect the devices. Participants with voice assistants and lighting less often believed that the chances of hacking these devices were low and less often cited trust in manufacturer compared to those with thermostats and security devices, respectively.

Actions:

- **Participants took a variety of security and privacy actions, with most being simplistic.** The four most common actions included: setting a password/PIN, limiting information entered in device app; not placing device in a private area; using two-factor authentication. There were several category differences, for example, participants with security devices were more likely to set a password/PIN than those with voice assistants.
- **Participants took more actions for their smart security devices.** The number of security and privacy actions taken by participants with security devices was significantly greater than that of participants with lighting, thermostats, and voice assistants.
- **Participants felt less able to protect their voice assistants.** They felt most able to protect the security and privacy of their security devices and sensors.
- **Participants expressed varied obstacles to taking action.** While the plurality of participants indicated that nothing prevents them from taking action because they are satisfied with what they've done, other frequently mentioned obstacles included: they don't understand security/privacy enough; manufacturers don't provide options; don't understand the device enough. There were several category differences, for example, thermostat and sensor participants more often said they were satisfied with what they've done.

Responsibility:

- **Participants viewed current responsibility for smart home security and privacy as being shared.** Responsibility was mostly assigned to themselves and manufacturers, with a minor role for government.
- **Participants believed manufacturers and the government should take on more responsibility.** While, for the most part, they believed personal responsibility was at an acceptable level, they indicated gaps in what manufacturers and the government are doing and should be doing.

Information Sources:

- **Current sources of smart home security and privacy information did not always align with preferred sources.** Manufacturer websites and product packages were frequently currently utilized and preferred. They would like to receive less information than they currently do from social media and family/friends and more from retailers.
- **Most participants indicated that smart home security and privacy information would likely inform their future purchases.** Participants with thermostats were least likely to report doing so.

- **Participants were generally willing to act on security and privacy information to protect their devices.** Over two-thirds said that they were willing to follow through on information about how to better secure their devices and home network and protect their privacy while using the devices.
- **Participants would be most trusting of security and privacy labels provided by the manufacturer or not-for-profit organizations.** They were least trusting of labels provided by for-profit organizations (other than the manufacturer) and the U.S. Government.

Takeaways

Based on the study results, we offer the following suggestions for developers of user-focused smart home security and privacy communications and education materials:

- **Emphasize that all types of devices may be at risk.** Tailor device-specific materials that communicate the likelihood and severity of risks as applicable. Emphasize that compromise of any device – even those viewed as less vulnerable or of less value – might lead to compromise of other, higher-value devices on the home network.
- **Clearly communicate security and privacy mechanisms.** Clearly detail the security and privacy features included in smart home products, what risks these address, and what options are user-configurable and recommended. Product security labels could provide a way for users to quickly find security and privacy information.
- **Encourage user action.** Be clear about the responsibilities consumers have in protecting their devices and data in easy-to-understand and actionable terms.
- **Target multiple communication channels.** Ensure education materials are distributed via multiple channels in a variety of formats consumable by different kinds of consumers, for example, those preferred by our study participants such as manufacturer websites, product packages, and online retailer websites.

INTRODUCTION

Internet of things (IoT) smart home devices – such as virtual voice assistants and smart speakers, smart thermostats, and smart security cameras -- offer a variety of benefits, including automation, convenience, physical security, and increased energy efficiency. Therefore, not surprisingly, adoption of smart home devices is on the rise. In 2024, an estimated 45% of U.S. households with internet had at least one device, and 18% had six or more devices [PARKS ASSOCIATES 2024]. These devices, while beneficial, introduce new aspects of device ownership needing to be addressed. Among these are smart home security and privacy, which are critical in light of the sensitive data that may be collected, or the physical impacts devices may have in the home environment.

The Importance of Consumer Education

While manufacturers are encouraged to build strong security and privacy mechanisms into their products, ultimately, the users (consumers) of smart home devices share some responsibility for protecting their devices and data. However, prior industry and research studies reveal that users may have inaccurate mental models[1] of smart home device security and privacy, express concerns even after adopting devices, struggle with the lack of transparency in data collection, and feel uncertain or powerless about being able to take protective actions [LAU 2018][TABASSUM 2019][ZENG 2017]. As a result, smart home device adoption may lag, user experience may suffer, and the devices and the data these collect may be vulnerable to compromise.

To help counter some of these issues, technology and research experts advocate for bringing more awareness about smart home security and privacy risks and actions via consumer education and communication efforts [HANEY 2020][LAU 2018][TABASSUM 2019]. In fact, current IoT security baselines, product label programs, and guidance from U.S. and international government [EU 2019][FCC 2024][NIST 2022], industry [CSDE 2019][IOTSF 2021] and standards [ETSI 2020] organizations recommend that manufacturers provide consumers with information about device security mechanisms and options. To be effective, consumer education should clearly communicate the IoT user's role in protecting their devices and proactively address typical consumer concerns, challenges, and misconceptions [ETSI 2020] [LAU 2018][NIST 2022][ZHENG 2018].

[1] A mental model is what a person believes about how something works. This belief may be accurate or inaccurate.

Addressing the Gaps in Smart Home Product Education

Security and privacy concerns and misconceptions may ultimately be influenced by the category (type) of device due to differences in functionality, data collection practices, and privacy and security mechanisms [EMAMI-NAEINI 2021][FASSL 2021]. For example, device categories with an audio capture and recording capabilities, such as virtual voice assistants, may be considered by users to be risky from a privacy perspective [MALKIN 2019].

However, there are few insights into how consumers' perspectives on smart home security and privacy differ depending on device category. A number of research groups (for example, [HANEY 2021][TABASSUM 2019][ZENG 2017]) have studied individuals' perspectives of smart home security and privacy using interviews. While interviews provide an in-depth look into the experiences of participating individuals, these inquiries typically involve few participants (usually 15-30) and may not reflect the broader population of U.S. adults. In addition, while there have been studies exploring users' software update attitudes for different types of devices [FASSL 2021][HANEY 2023], few studies directly compare consumers' broader security and privacy perceptions for a breadth of widely-adopted device categories.

The lack of understanding about category differences – as perceived by individuals throughout the U.S. -- leaves the smart home community at a disadvantage in knowing how to focus user education efforts to address device-specific issues. Therefore, consumers may remain uninformed or lack motivation to protect device categories they consider less valuable, leaving their devices and data vulnerable.

To address this shortfall, we surveyed 401 active users (adopters) of smart home devices. While smart home non-adopters may have their own set of security and privacy concerns that discourage them from engaging with these technologies, we focused specifically on active users of these devices. This focus allowed us to gain an understanding of their perceptions and actions after directly interacting with and experiencing the benefits of these devices.

Our survey study sought to answer the following questions:

- How do users' perceptions about the security and privacy of their smart home devices differ across device categories, if at all?
- How do users' security and privacy actions and perceptions about taking action differ across device categories, if at all?
- How do users' perceptions of who is responsible for smart home security and privacy differ across device categories, if at all?
- From which information sources do users currently and prefer to receive smart home security and privacy information?
- What is the likelihood that security and privacy information will influence users' smart home purchases and actions?

Audience

The identification of differences across devices can inform smart home device manufacturers and security label programs to go beyond generic guidance by tailoring education materials to address the specific risks, security and privacy features, and expected user protective actions for individual device categories. In addition, users of smart home devices may benefit through awareness of common misconceptions and their own responsibility in protecting their smart homes.

Related Publication

This report details results from the full smart home survey. The following paper – written for a research audience – reports a subset of the results contained here:

Haney, J.M., Acar, Y., Li, A., & Haney, F. (2025). Smart Home Users' Security and Privacy Perceptions and Actions Differ By Device Category: Results from a U.S. Survey. *Proceedings of the International Conference on Human-Computer Interaction (HCII)*. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=957194

WHAT WE DID

To understand smart home users' security and privacy perceptions and behaviors, we surveyed 401 smart home users. Our study followed ethical research guidelines and was approved by the NIST Research Protections Office.

In this section, we provide a high-level overview of our research process. A detailed description of the study methodology is included in the Technical Appendix.

Survey Topics

We focused the survey to explore participants' perceptions and behaviors related to five smart home device categories of particular interest:

Lighting devices (e.g., smart light bulbs and lighting systems) - allow for automating lighting patterns and brightness for convenience or safety.

Security devices (e.g., smart door locks, smart security cameras, video doorbells) - contribute to the physical security and safety of the home.

Sensors (e.g., smart smoke detectors, water leak sensors) - monitor and alert based on physical conditions of the home, often with a safety purpose.

Thermostats (e.g., Google Nest, Ecobee) - allow users to adjust and automate home temperature settings, often for energy efficiency.

Voice assistants (e.g., Amazon Echo, Apple HomePod Mini, Google Home) - carry out tasks via voice command, may act as an interface with other smart home devices.

We selected these categories since they are among the most popular in the U.S., represented varying levels of sophistication, and collected different types of data.

The survey (see Technical Appendix for the survey instrument) addressed the following topics:

- perceptions about device security/privacy
- level of security and privacy concern
- reasons for lack of concern or using smart home devices despite concerns

- any security and privacy actions participants took to protect their devices and how effective participants believed those actions to be
- perceived ability to protect the security and privacy of devices and the data those collect
- perceived barriers to taking action to protect device security and privacy
- perceptions about how much responsibility participants, device manufacturers, and the U.S. Government have for smart home security and privacy
- current and preferred sources for information on smart home security and privacy
- likelihood of security and privacy information informing future smart home purchases or resulting in taking action
- trust of security and privacy labels provided by different entities
- participant demographics

Participant Recruitment and Data Collection

Participants were recruited from the Prodege opt-in research panel to be representative of the adult (18+ years of age) U.S. population. To be eligible for the survey, participants had to be active users of a smart home device in at least one of the five categories of interest.

Participants answered the survey for just one device category they used based on a random assignment. For example, if a participant indicated at the start of the survey that they had a smart thermostat and a smart security device, they may have been asked to answer the survey based on their thoughts and experiences only for their thermostat.

Survey data were collected via an online survey platform for two weeks in February 2022. Responses were anonymized. About 80 participants completed the survey for each smart home device category: 82 for lighting, 80 for security devices, 80 for sensors, 80 for thermostats, and 79 for voice assistants.

Data Analysis

We analyzed the survey data using two types of statistics. First, we calculated descriptive statistics that summarize participant responses for each question. For example, we report the percentage of participants who said they were extremely concerned about the security of their voice assistants. Second, we used statistical analysis methods to determine whether there were significant differences in participants' responses across device categories. For example, we report that participants taking the survey about their voice assistants were significantly – from a statistical perspective -- more concerned about their device's security as compared to participants indicating concern for their smart lighting devices.

Throughout the report, we use call-out boxes to note any results that, statistically speaking, indicate significant differences across smart home device categories. Detailed statistical results can be found in the Technical Appendix.

PARTICIPANTS AND DEVICES

In this section, we provide an overview of the survey participants and their smart home device usage. Additional details on participants can be found in the Technical Appendix.

Participants used a variety of smart home devices, with voice assistants being the most common.

While participants answered the survey based on just one smart home device category, they also indicated which of the five types of devices they used (Fig. 1). Over half had voice assistants, while more than 35% used smart security devices, lighting, sensors, and thermostats. Additionally, 51% had devices in more than one category, and 8% used devices in all five categories.

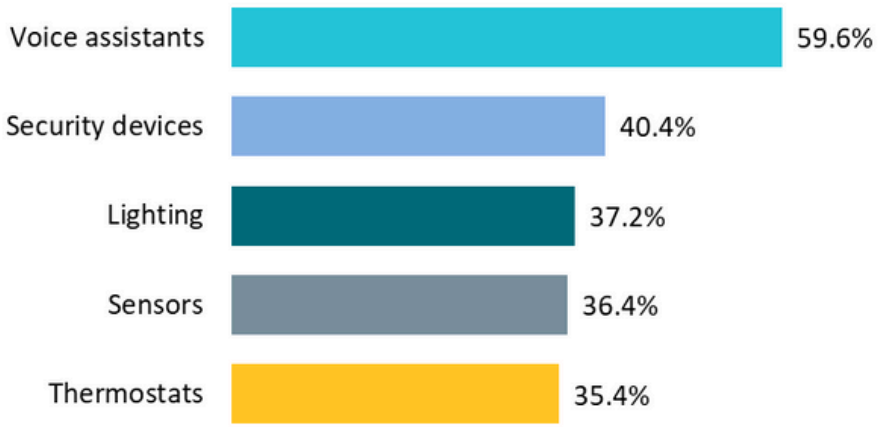


Figure 1. Percentage of the 401 participants using smart home devices in each device category

Participants represented various demographic groups.

The 401 participants were near-representative of the U.S. population with respect to age group, education level, race, ethnicity, and sex (Table 1). See the Technical Appendix for more details on the participants (state of residency, home ownership) and how the participant demographic groups compared to the U.S. adult population.

Table 1: Demographic data of 401 survey participants

Variable	Groups	Number	Percentage
Age Range (years)	18 - 34	150	37.4%
	35 - 54	125	31.2%
	55+	120	29.9%
	No answer	6	1.5%
Race	White	256	63.8%
	Black	60	15.0%
	Asian	39	9.7%
	Pacific Islander	5	1.2%
	American Indian	11	2.7%
	Multi-racial	16	4%
	No answer	14	3.5%
Ethnicity	Not Hispanic/Latino	296	73.8%
	Hispanic/Latino	99	24.7%
	No answer	6	1.5%
Education level	High school diploma and lower	126	31.4%
	Some college and Associate's degree	116	28.9%
	Bachelor's degree and higher	152	37.9%
	No answer	7	1.7%
Sex	Female	218	54.4%
	Male	178	44.4%
	No answer	5	1.2%

Participants took on different roles for their smart home devices.

Over half of participants (58%) were smart home administrators who were responsible for device installation and troubleshooting. 39% were active smart home users, but not administrators. Finally, 3% selected “Other” or no response for smart home role.

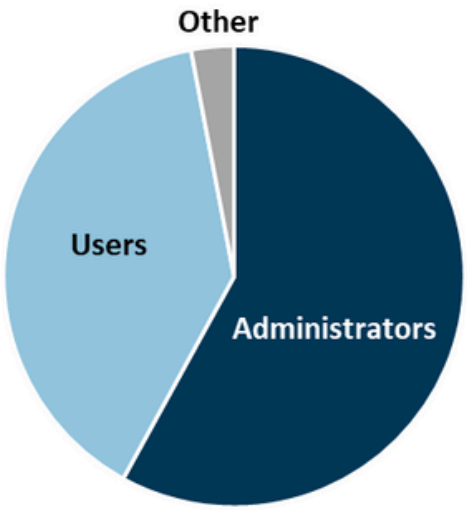


Figure 2. Participants’ roles with respect to their smart home devices

SECURITY AND PRIVACY PERCEPTIONS

To gauge participant perceptions that could act as motivations or barriers to smart home security and privacy actions, we asked participants questions about their:

- perceptions of device security and privacy
- perceived level of understanding of security and privacy risks
- level of security and privacy concerns
- level of concern for specific security and privacy risk scenarios
- reasons for lack of concern or continued use of devices despite having concerns

Participants rated voice assistants as least secure and privacy protecting.

Participants rated their level of agreement with the following two statements on a 5-point scale ranging from “Strongly disagree” to “Strongly agree”:

- “I think that most of these smart home devices are secure.” (Fig. 3)
- “I think that most of these smart home devices protect my privacy.” (Fig. 4)

Participants most often agreed or strongly agreed that their smart security devices were **secure** (80%) and **privacy-protecting** (70%), followed by sensors (70% security, 61% privacy). Participants with voice assistants had the lowest agreement levels for both security (35%) and privacy (39%).

Participants believed their ***voice assistants*** were significantly less secure and privacy-respecting than all other device categories.

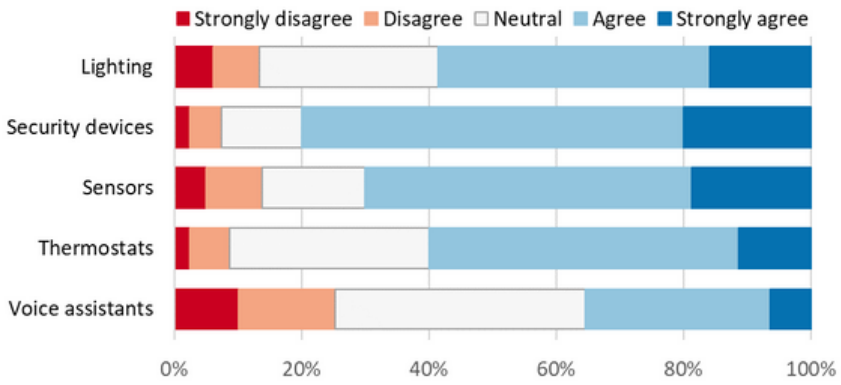


Figure 3. Participants’ level of agreement that their smart home devices were **secure**

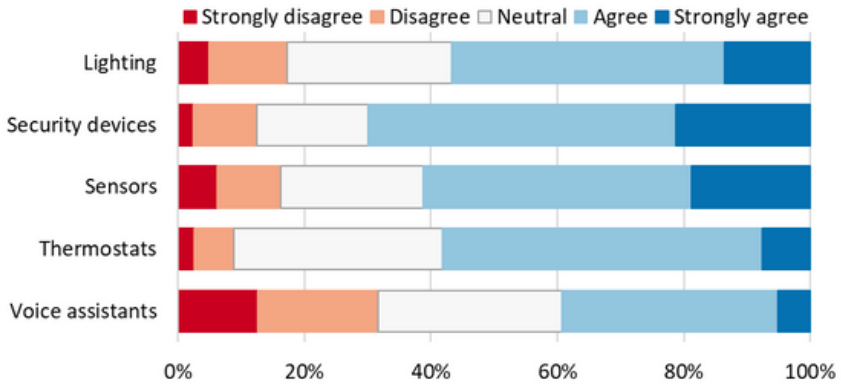


Figure 4. Participants’ level of agreement that their smart home devices were **privacy-protecting**

Participants generally believed they understood the security and privacy risks of their smart home devices.

Participants rated their level of agreement with the following two statements on a 5-point scale ranging from “Strongly disagree” to “Strongly agree”:

- “I understand the security risks associated with my smart home device.” (Fig. 5)
- “I understand the privacy risks associated with my smart home device.” (Fig. 6)

Participants most often agreed or strongly agreed that they understood **security** risks for smart security devices (73%) and sensors (65%). They less often agreed for voice assistants (43% agreed/strongly agreed). For **privacy**, participants most often said they understood risks for sensors (69%) and security devices (68%). They least often understood the privacy risks for voice assistants (52%).

Participants thought they had much less understanding of security risks for ***voice assistants*** than they did for ***security devices***.

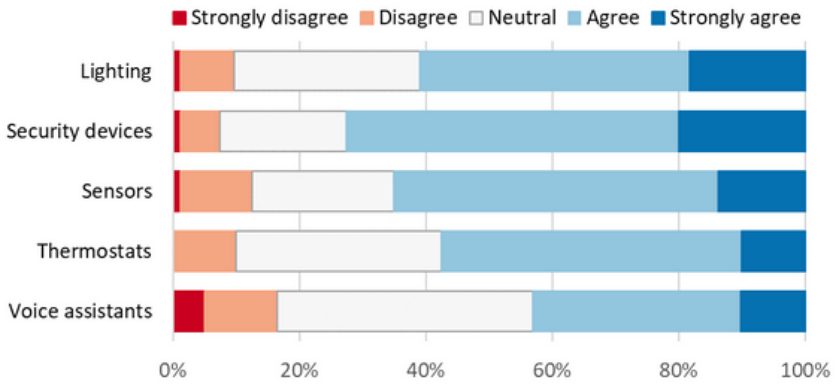


Figure 5. Participants’ level of agreement that they understood the **security** risks of their devices

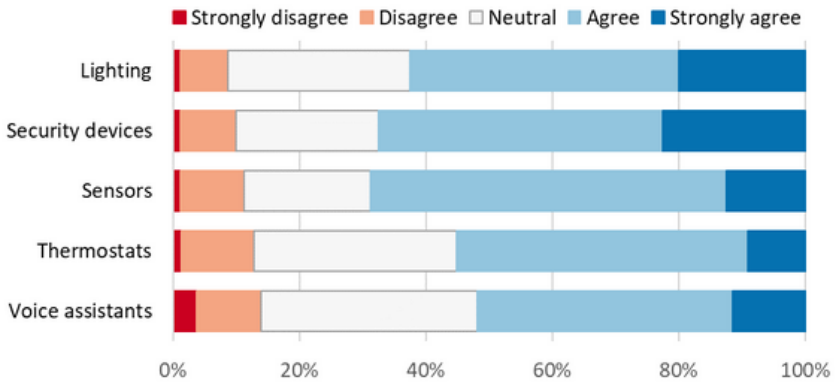


Figure 6. Participants’ level of agreement that they understood the **privacy** risks of their devices

A majority of participants were concerned about the security and privacy of their devices.

Participants rated their level of concern about the security and privacy of their smart home devices.

The majority of participants – ranging from 70% for voice assistants to 53% for security devices – were at least somewhat concerned about the **security** of the devices (Fig. 7). Concern levels for **privacy** were similar, ranging from 73% for voice assistants to 54% for security devices being at least somewhat concerned (Fig. 8). Over 20% were moderately or extremely concerned for all categories.

We found that participants' views that voice assistants were less secure and privacy-protecting did not translate into higher overall levels of security and privacy concern. However, few participants with voice assistants indicated that they were not at all concerned (9% for security, 5% for privacy).

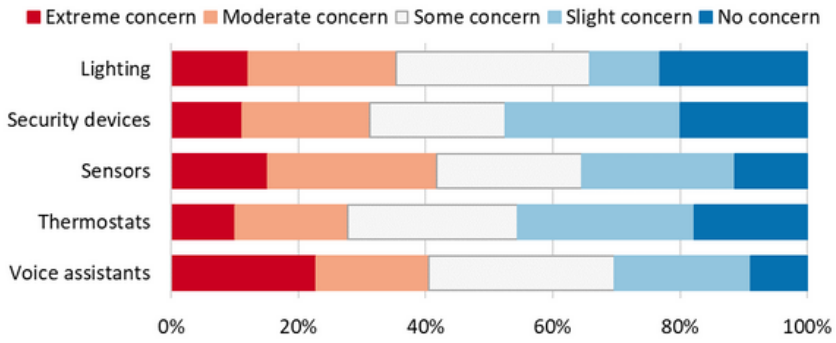


Figure 7. Participants' level of concern about the **security** of their devices.

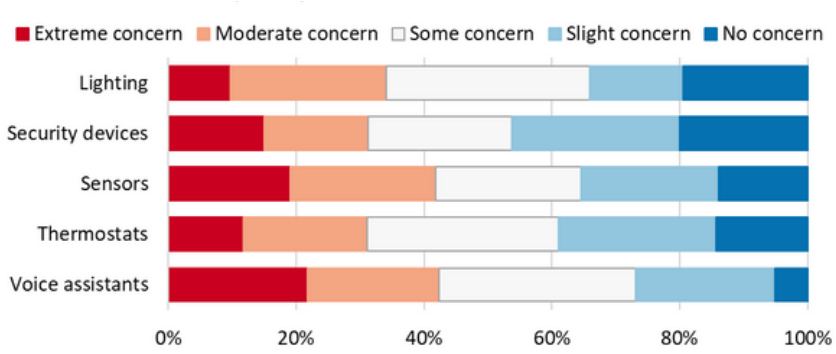


Figure 8. Participants' level of concern about the **privacy** of their devices.

Over half of participants expressed at least some concern about potential problematic security and privacy scenarios.

In addition to eliciting general concern levels, participants rated their level of concern for three specific security scenarios (scenarios S1 - S3 in Fig. 9) and 10 privacy scenarios (scenarios P1 - P10 in Fig. 10). The privacy scenarios were based on items in the NIST Catalog of Problematic Data Actions and Problems, an illustrative set of "problems that individuals could experience as the result of data processing or their interactions with systems, products, or services."

For the three **security** scenarios, between 65% and 69% of participants were at least somewhat concerned, and 38% to 42% were moderately or extremely concerned. For all **privacy** scenarios, over half were at least somewhat concerned, ranging from 60% to 71%. Participants expressed the highest levels of concern at about 46% moderately/extremely concerned for P1 (having to provide more personal/private information than is comfortable), P2 (tracking of data or usage in a manner violating individual rights), P5 (combining of data to reveal private things about household members), and P8 (tracking of data or usage in a manner resulting in physical harm).

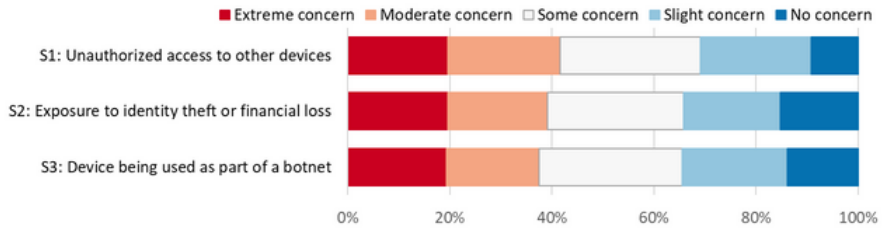


Figure 9. Participants' level of concern about **security** scenarios with potential for negative consequences. The term "botnet" was defined.

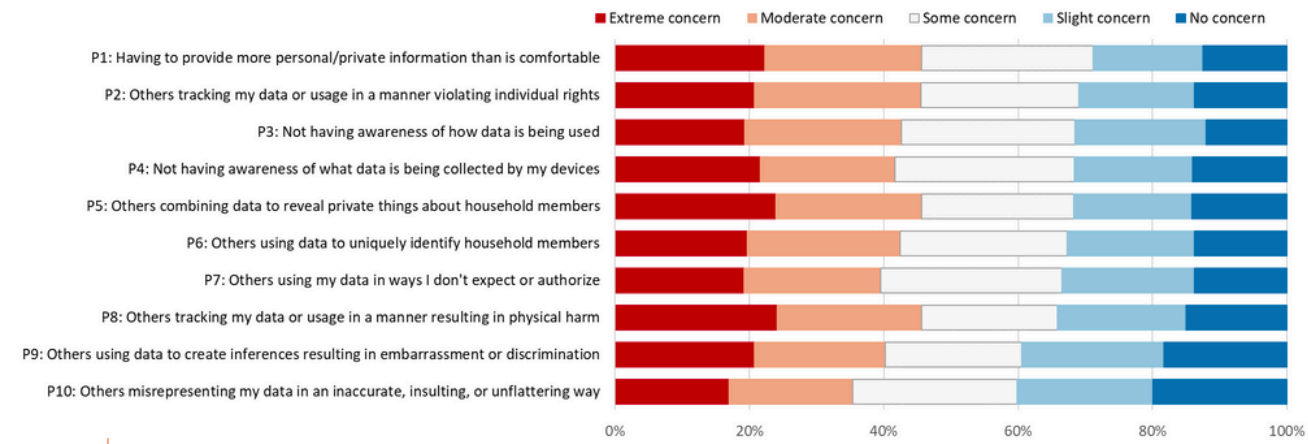


Figure 10. Participants' level of concern about **privacy** scenarios with potential for negative consequences

Participants had varying beliefs about security and privacy which, in part, could explain their levels of concern.

Participants selected reasons why they either 1) had little or no security or privacy concerns or 2) continued to use their devices even if concerned (Fig. 11).

Each reason was selected by fewer than 40%. Participants most frequently believed that the benefits of having their smart home devices outweighed any security or privacy risks (38%). The other most-selected options included a belief that their data or devices were not interesting enough for bad actors to target (31%) and that the chances of their devices being hacked were low (31%).

Participants with ***thermostats*** were more likely to believe that the chances of their devices being hacked were low compared to participants with smart ***lighting*** and ***voice assistants***.

Participants with ***sensors*** more often thought that their actions alleviated their concerns than those with ***thermostats***.

Participants with smart ***security devices*** more often said that they trusted the manufacturer to protect their privacy as compared to participants with ***lighting*** and ***voice assistants***.

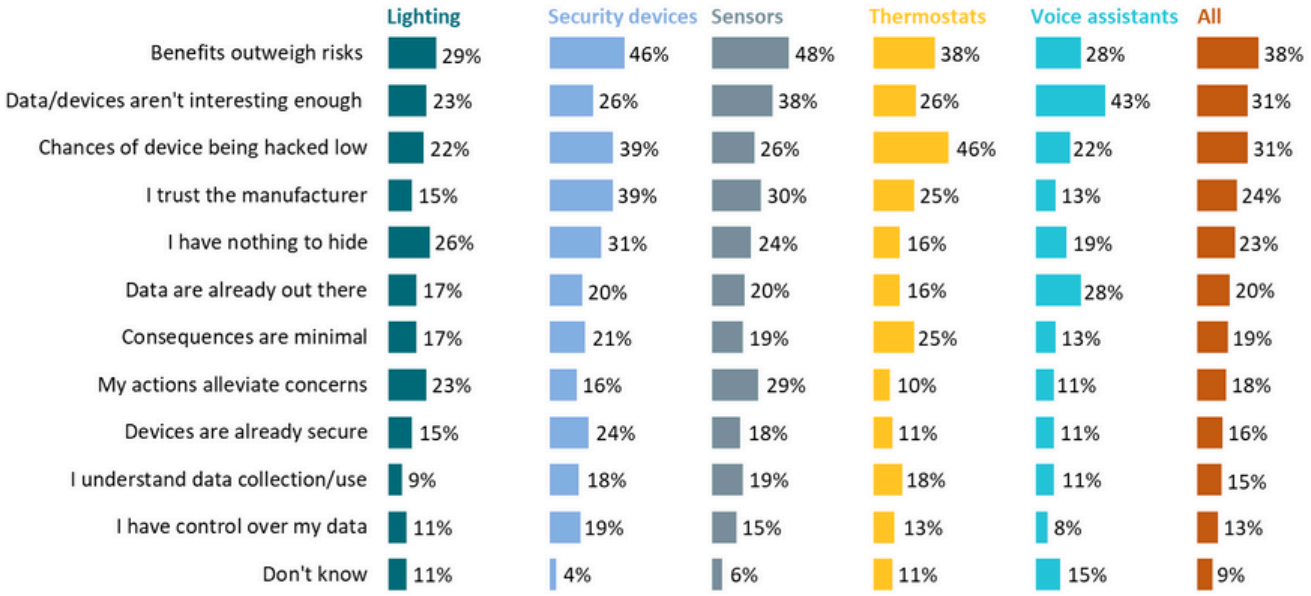


Figure 11. Participants' reasons for lack of concern or continued use of smart home devices despite being concerned by device category

ACTIONS

To gain insight into if and how participants attempt to secure their smart home devices and protect their privacy while using their devices, we asked participants questions about:

- security and privacy actions they take for their smart home devices
- security and privacy actions they take for their home network
- perceptions of how much their actions alleviate their concerns
- perceived ability to take action
- willingness to take action
- barriers to taking action

Participants took a variety of security and privacy actions, with most being simplistic.

Participants selected the actions they took to secure and protect the privacy of their smart home devices and data (Fig. 12). No actions were selected by a majority. Participants most-frequently said they set a password or PIN on their device or device 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 who indicated that they take "other actions" said that they disconnect their devices.

Participants with ***security devices*** more often set a password or PIN compared to participants with smart ***lighting*** or ***voice assistants***.

Participants with ***voice assistants*** less often set up or changed security or privacy options compared to those with devices in ***all other categories***.

Participants with ***thermostats***:

- less often take care not to place their devices in sensitive or private areas of the home compared to participants with ***security devices*** and ***voice assistants*** and
- less often said they were careful about what they say or do near their devices than participants with devices in ***all other categories***.

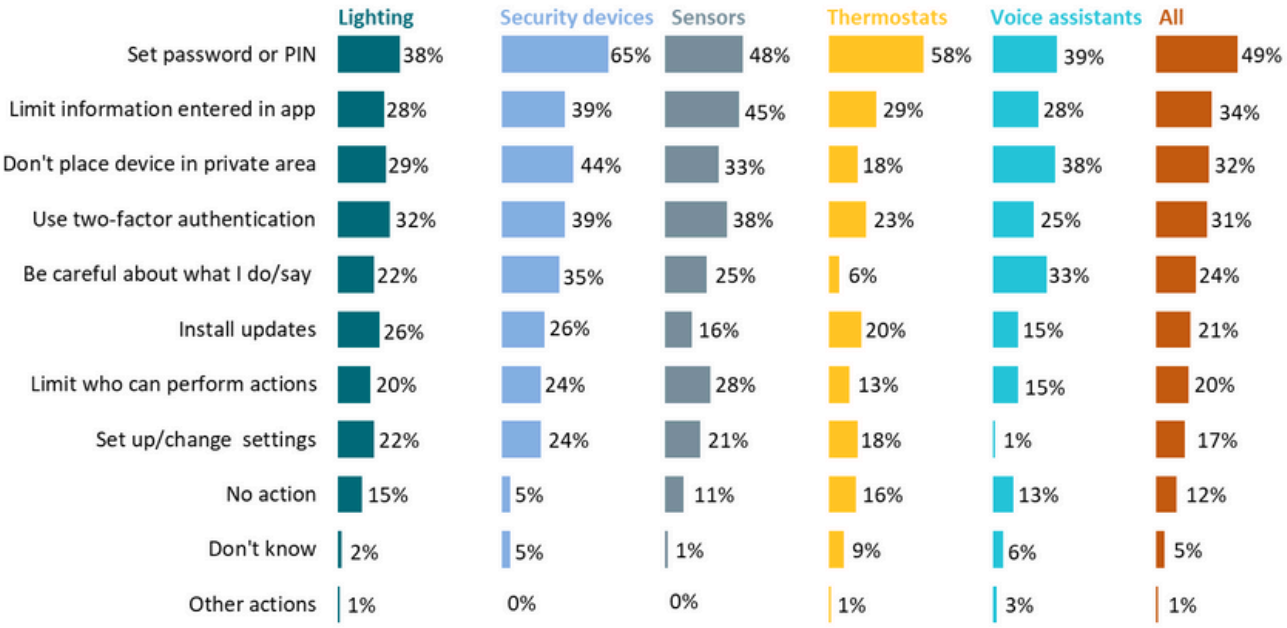


Figure 12. Participants' smart home security and privacy actions by device category

Participants took more actions for smart security devices.

Participants took an average of 2.3 actions. 17% of participants took no action, 21% took just one action, and the plurality (41%) took 2 or 3 actions. A breakdown of the percentages of number of actions per device category is shown in Fig. 13.

Participants with ***security devices*** (3.0 actions on average) took significantly more actions as compared to those with smart ***lighting*** (2.2 actions on average), ***voice assistants*** (2.0 actions), and ***thermostats*** (1.8 actions).

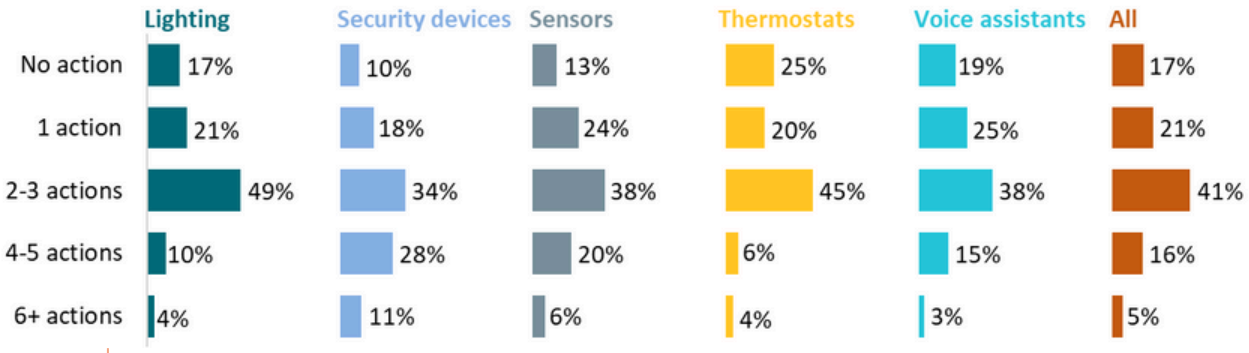


Figure 13. Number of smart home device security and privacy actions by device category

To protect their home networks, participants most often set a Wi-Fi password.

The security of a home network can directly impact smart home devices. Therefore, we asked participants which actions they took to protect their home network (Fig. 14).

Almost two-thirds of participants said that they set a password for their home Wi-Fi. All other actions were selected by about a quarter or less of participants. Just 8% said they did not take any actions on their home network.

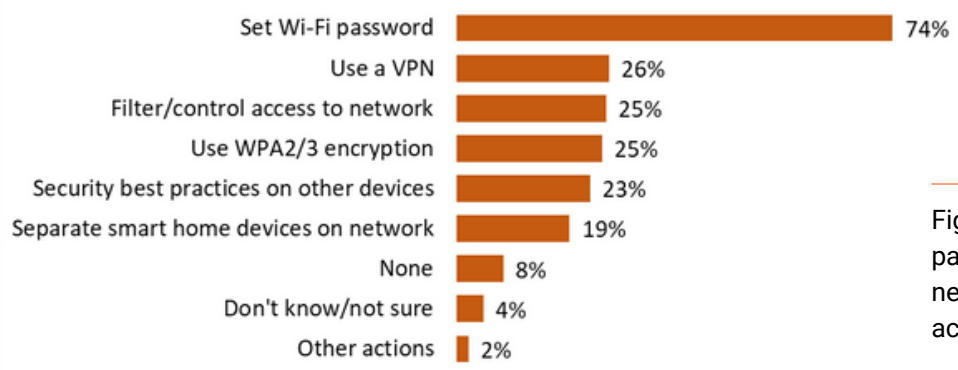


Figure 14. Percentage of participants taking home network security and privacy actions

The majority of participants thought their actions helped alleviate their security and privacy concerns.

For each security or privacy action they selected, participants were asked to rate their level of agreement with the statement "This action decreases my security and privacy concerns for my <*device category*>" (Fig. 15).

Over 70% of participants agreed or strongly agreed that all actions decreased their concerns. Participants were most confident in two-factor authentication (89% agree/strongly agree), setting a Wi-Fi password (86%), using WPA2/3 encryption for their home Wi-Fi (86%), and filtering or controlling access to their home network (85%).

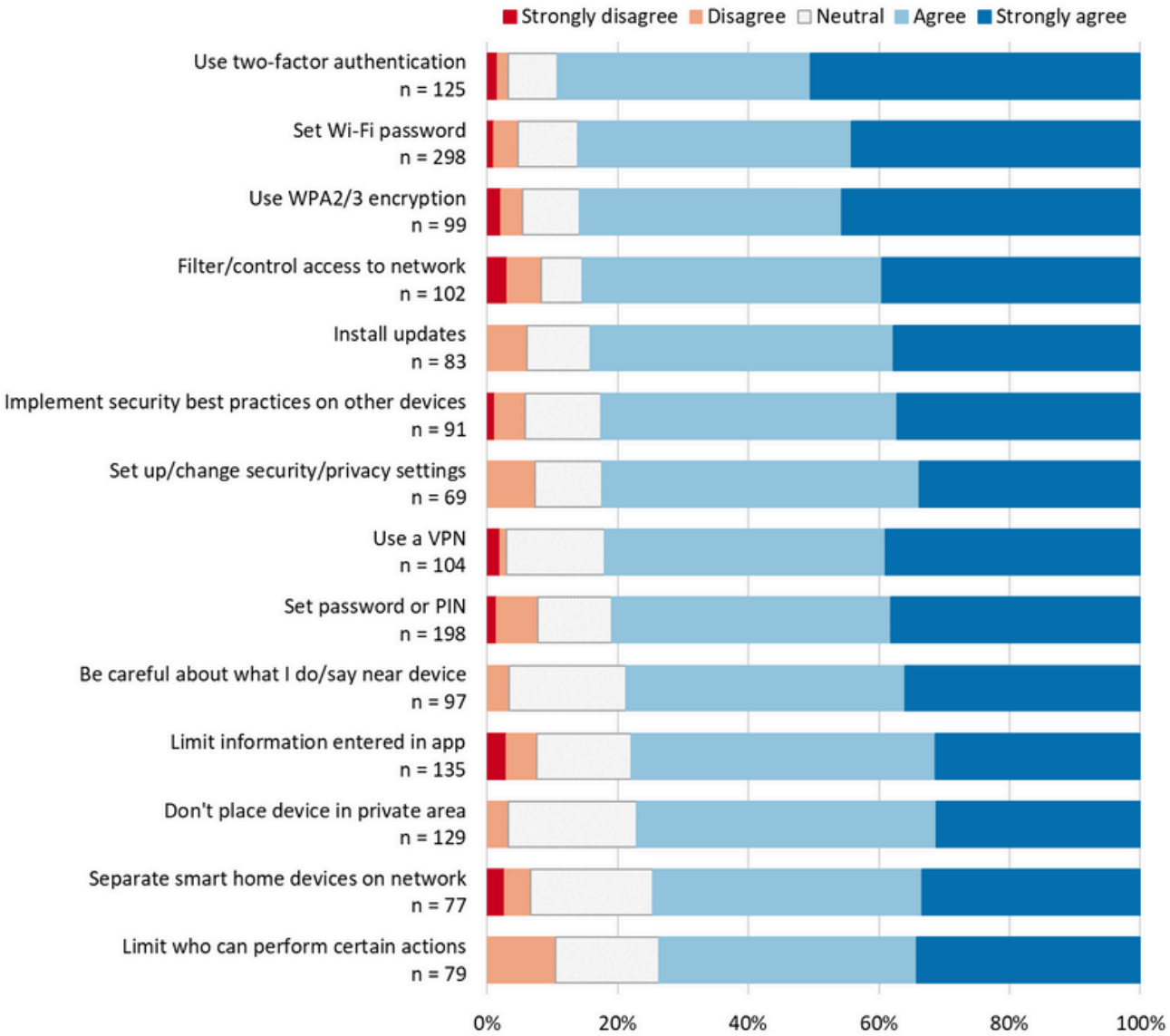


Figure 15. Participants' level of agreement that their actions decrease their security and privacy concerns.

Participants felt less able to protect their voice assistants.

Participants rated their level of agreement with the following two statements on a 5-point scale ranging from “Strongly disagree” to “Strongly agree”:

- “I feel able to protect my smart home device’s security.” (Fig. 16)
- “I feel able to protect my privacy when using my smart home device.” (Fig. 17)

Over half of participants agreed or strongly agreed with each statement for all smart home device categories with the exception of voice assistants for which only 37% agreed for both the security and privacy statements.

Participants with ***voice assistants*** felt significantly:

- less able to protect device security compared to participants with smart ***security devices*** and
- less able to protect their privacy as compared to those with devices in ***all other categories***.

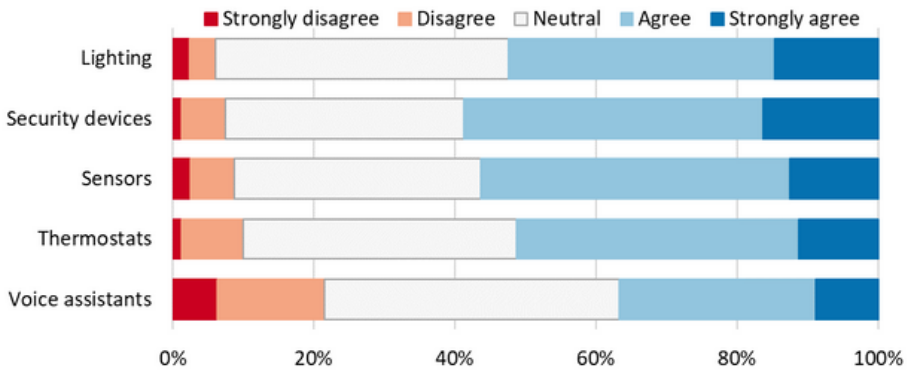


Figure 16. Participants’ level of agreement that they felt able to protect their smart home device’s **security**.

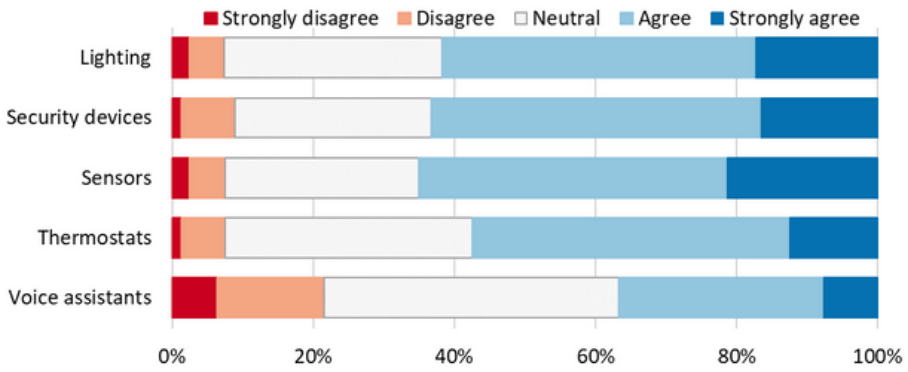


Figure 17. Participants’ level of agreement that they felt able to protect their **privacy** when using their smart home device.

Most participants were willing to put effort into protecting their devices.

Participants rated their level of agreement with the following two statements on a 5-point scale ranging from “Strongly disagree” to “Strongly agree”:

- “I am willing to put in the effort to secure my smart home device.” (Fig. 18)
- “I am willing to put in the effort to protect my privacy when using my smart home device.” (Fig. 19)

Over two-thirds of participants agreed or strongly agreed with each statement for all smart home device categories. Participants with smart sensors were most willing (78% agreed/strongly agreed), and those with voice assistants were least willing (61%). However, the overall differences in ratings across device categories were not statistically significant.

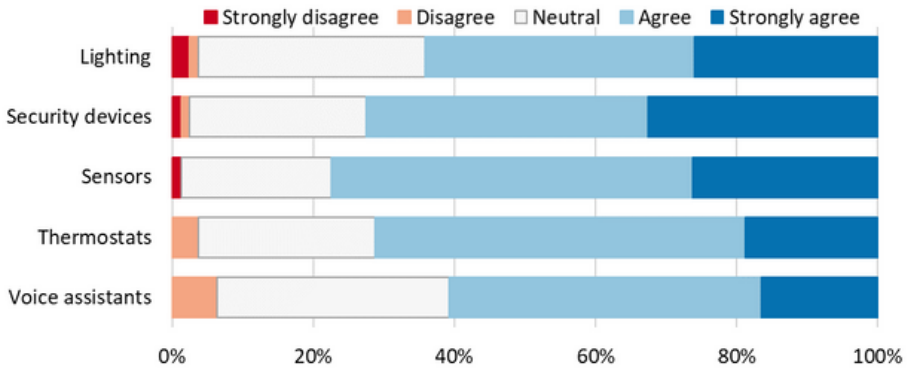


Figure 18. Participants’ level of agreement that they were willing to put effort into **securing** their smart home device.

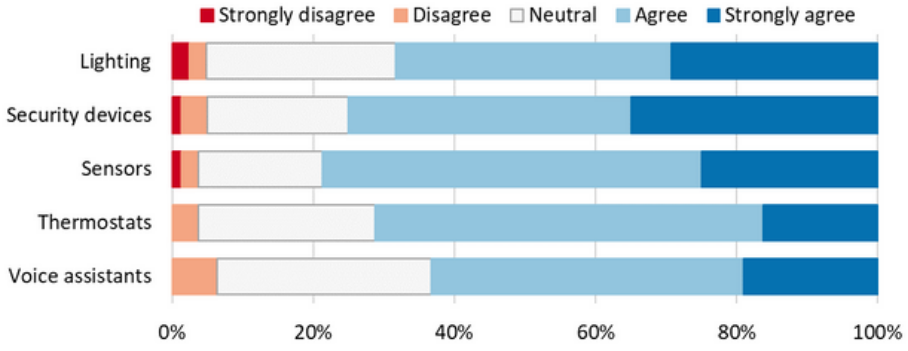


Figure 19. Participants’ level of agreement that they were willing to put effort into **protecting their privacy** when using their smart home device.

Participants expressed varied obstacles to taking action.

Participants indicated barriers that keep them from taking action or more action than they already take to ease their security concerns (Fig. 20). Then, they selected barriers that keep them from taking action to ease their privacy concerns (Fig. 21).

Less than 30% of participants selected each barrier. Most commonly, 27% of participants for security and 28% for privacy said that nothing prevents them because they are satisfied with the actions they had already taken. Next, 23% and 20% said that they do not understand device security or privacy, respectively. In addition, for privacy, 20% indicated that there are were not enough options for configuring their privacy preferences. For both security and privacy, 9% said that nothing prevents them because they are not concerned.

For security obstacles, participants with ***voice assistants*** indicated that nothing prevents them because they were satisfied with the actions they had already taken less often compared to those with ***thermostats***.

For privacy, participants with ***thermostats***:

- more often said that nothing prevents them because they were satisfied with the actions they had already taken, as compared to those with ***voice assistants***, ***security devices***, and smart ***lighting*** and
- less often indicated that there are no options for setting their privacy preferences than participants with smart ***lighting***.

For privacy, participants with ***sensors*** said that nothing prevents them because they were satisfied with the actions they had already taken, as compared to those with ***voice assistants***.

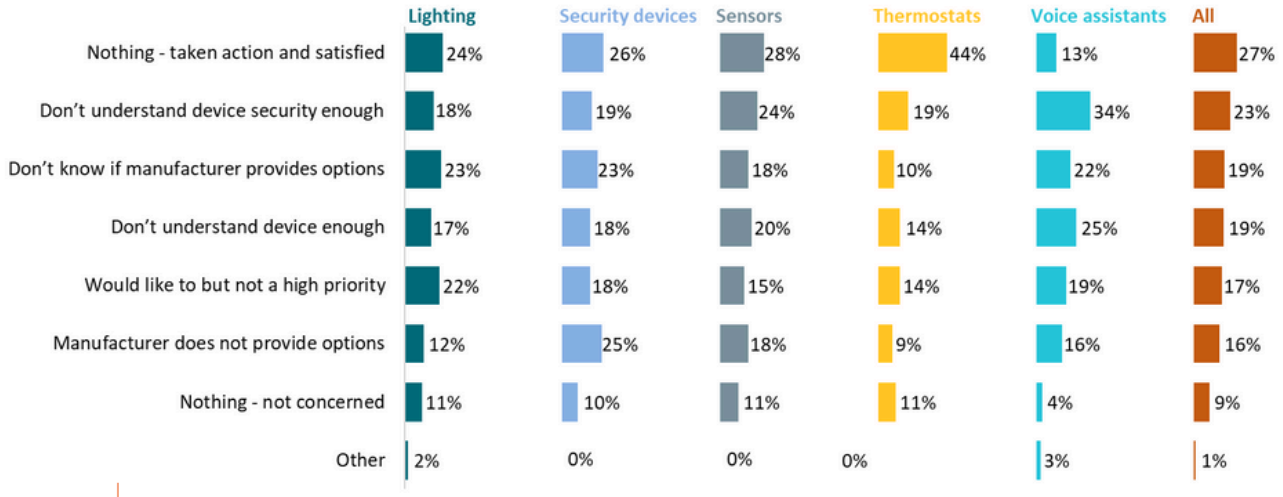


Figure 20. Percentages of participants selecting **security** action barriers by device category

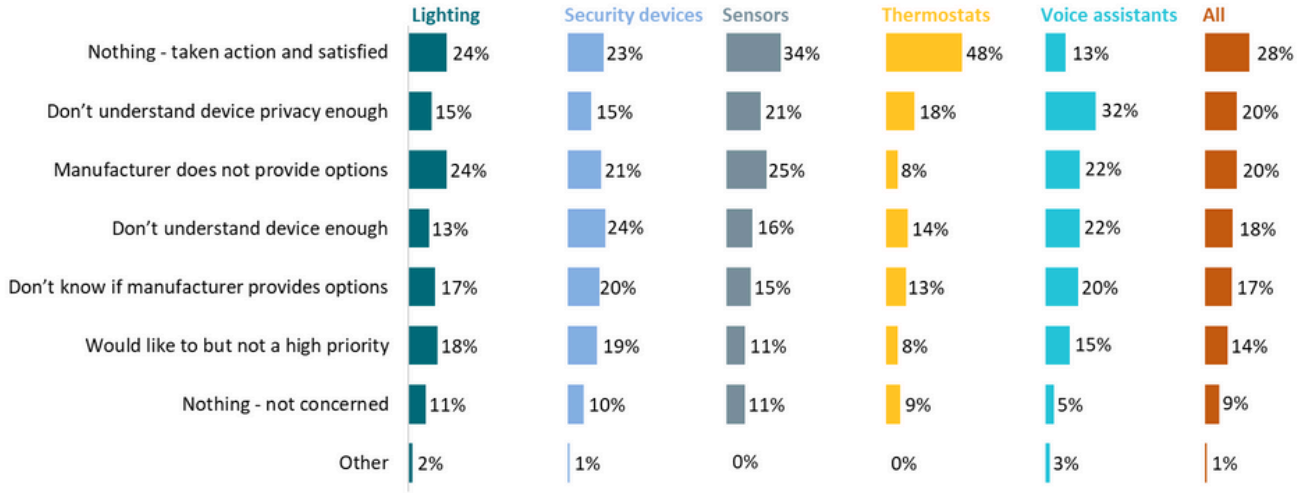


Figure 21. Percentages of participants selecting **privacy** action barriers by device category

RESPONSIBILITY

To gain insight into who participants thought was responsible for the security and privacy of their smart home devices, we asked participants questions about:

- current and ideal personal responsibility
- current and ideal manufacturer responsibility
- current and ideal government responsibility

Participants viewed current responsibility for smart home security and privacy as being shared.

Participants indicated their perceptions of how much responsibility that they, manufacturers, and the government *currently* have for the security and privacy of their smart home devices on a 5-point scale from "Not at all responsible" to "Completely responsible." Fig. 22 and Fig. 23 show the ratings per smart home device category. Over half of participants (57% security, 56% privacy) assigned responsibility to all three entities, with 92% assigning responsibility to at least two.

Between 53% (thermostats) and 74% (sensors) believed that they were mostly or completely personally responsible for device **security**. There were similar ratings for **privacy**, ranging from 56% (thermostats) to 73% (sensors) mostly or completely personally responsible.

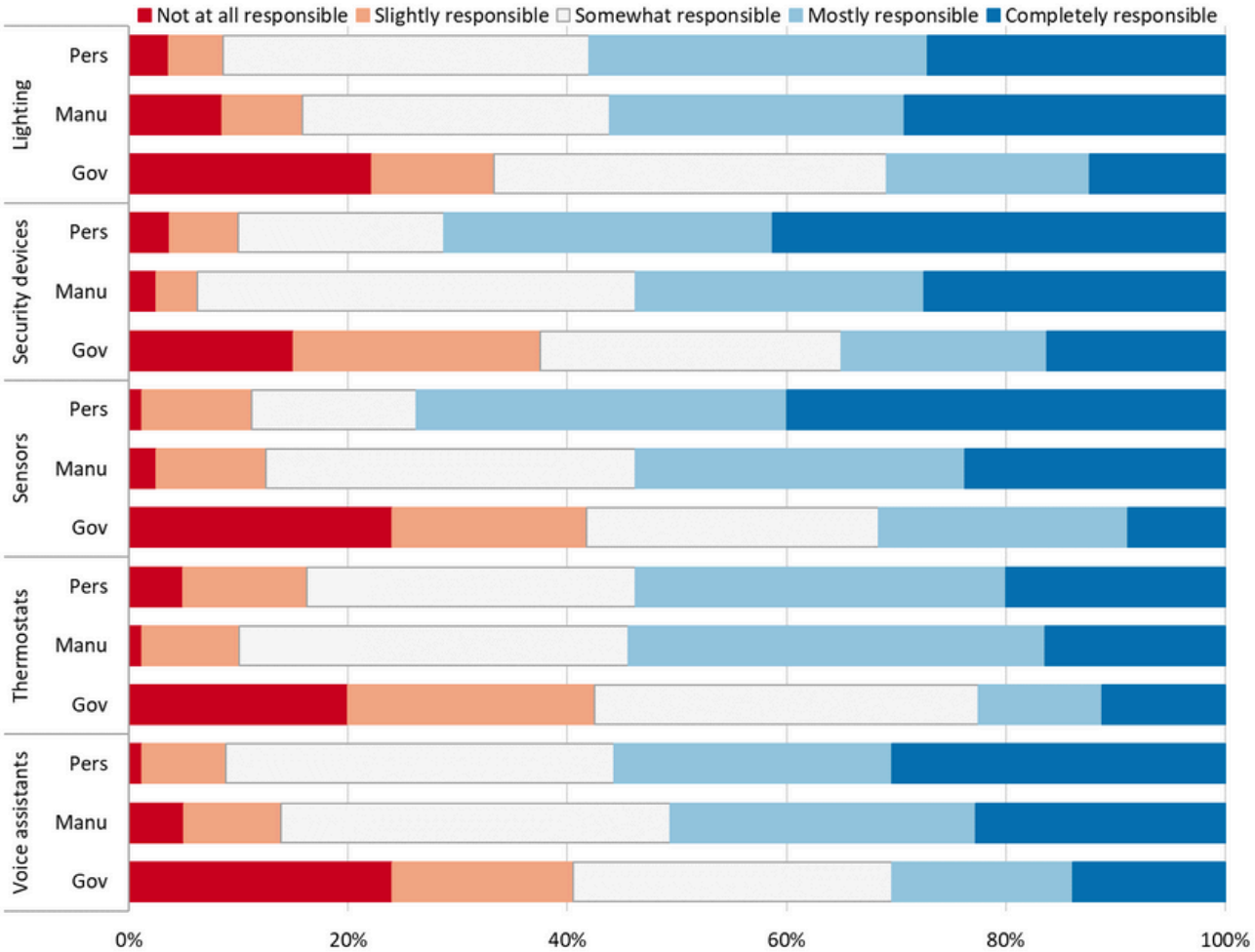


Figure 22. Participants' ratings of **current security** responsibility.
Pers = Personal responsibility
Manu = Manufacturer responsibility
Gov = Government responsibility

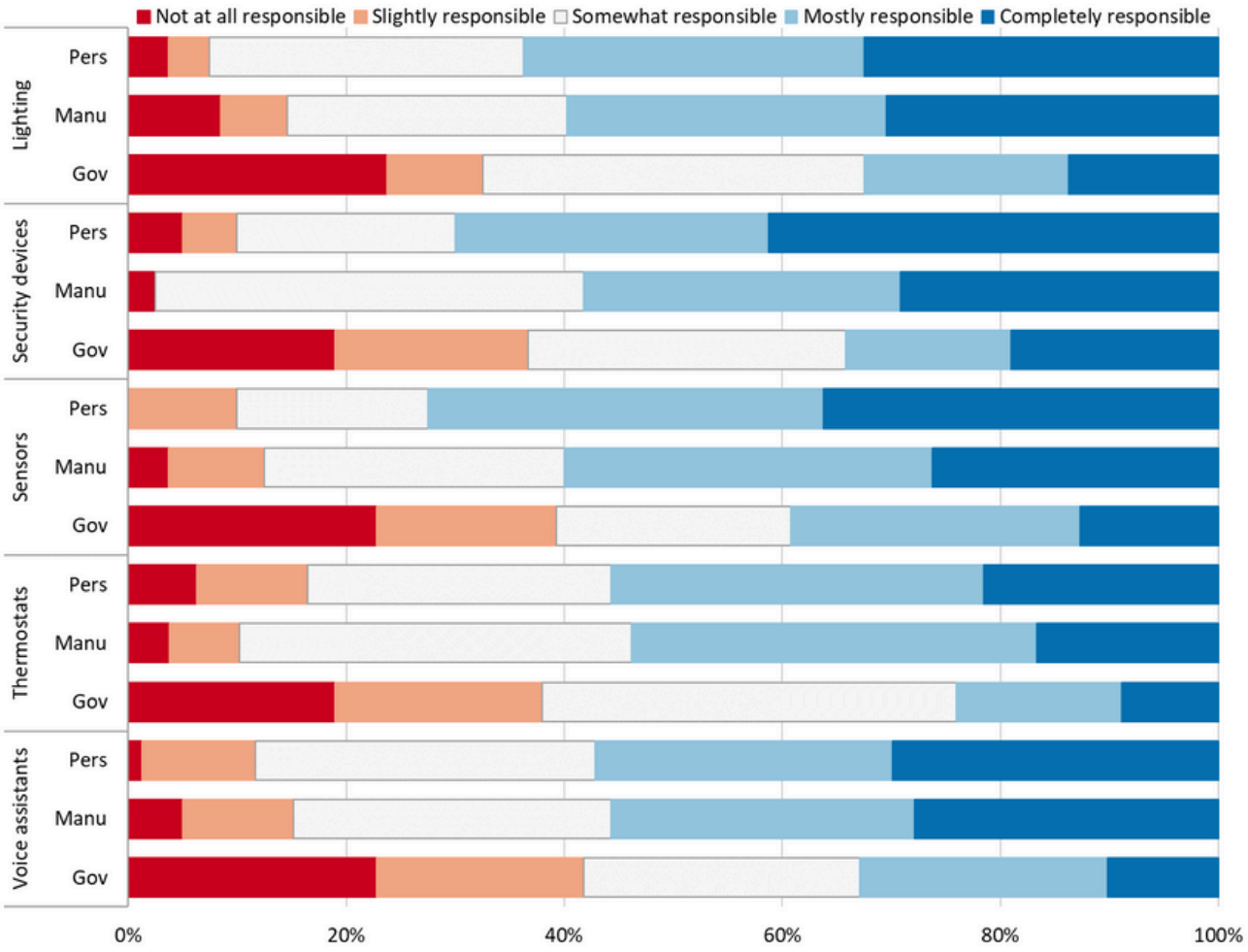


Figure 23. Participants' ratings of **current privacy** responsibility.
Pers = Personal responsibility
Manu = Manufacturer responsibility
Gov = Government responsibility

Ratings of manufacturer responsibility for security ranged from 51% (voice assistants) to 56% (lighting) mostly or completely responsible. Between 54% (thermostats) and 60% (lighting and sensors) of participants thought manufacturers were mostly/completely responsible for device privacy.

Between 23% (thermostats) and 35% (security devices) thought the government was currently mostly or completely responsible for smart home **security**. For **privacy**, between 24% (thermostats) and 39% (sensors) thought the **government** was mostly/completely responsible.

Participants assigned significantly less personal **security** responsibility for ***thermostats*** compared to ***security devices*** and ***sensors.***

Participants believed manufacturers and the government should take on more responsibility.

Participants indicated their perceptions of how much responsibility that they, manufacturers, and the government *ideally* should have for the security and privacy of their smart home devices on a 5-point scale from "Not at all responsible" to "Completely responsible." Fig. 24 and Fig. 25 show the ratings per smart home device category. Over half of participants (66% security, 64% privacy) assigned responsibility to all three entities, with 96% assigning security responsibility and 95% assigning privacy responsibility to at least two.

Between 56% (lighting) and 76% (sensors) believed that they ideally should be mostly or completely personally responsible for device **security**. **Privacy** ratings were similar, ranging from 58% (lighting) to 76% (sensors).

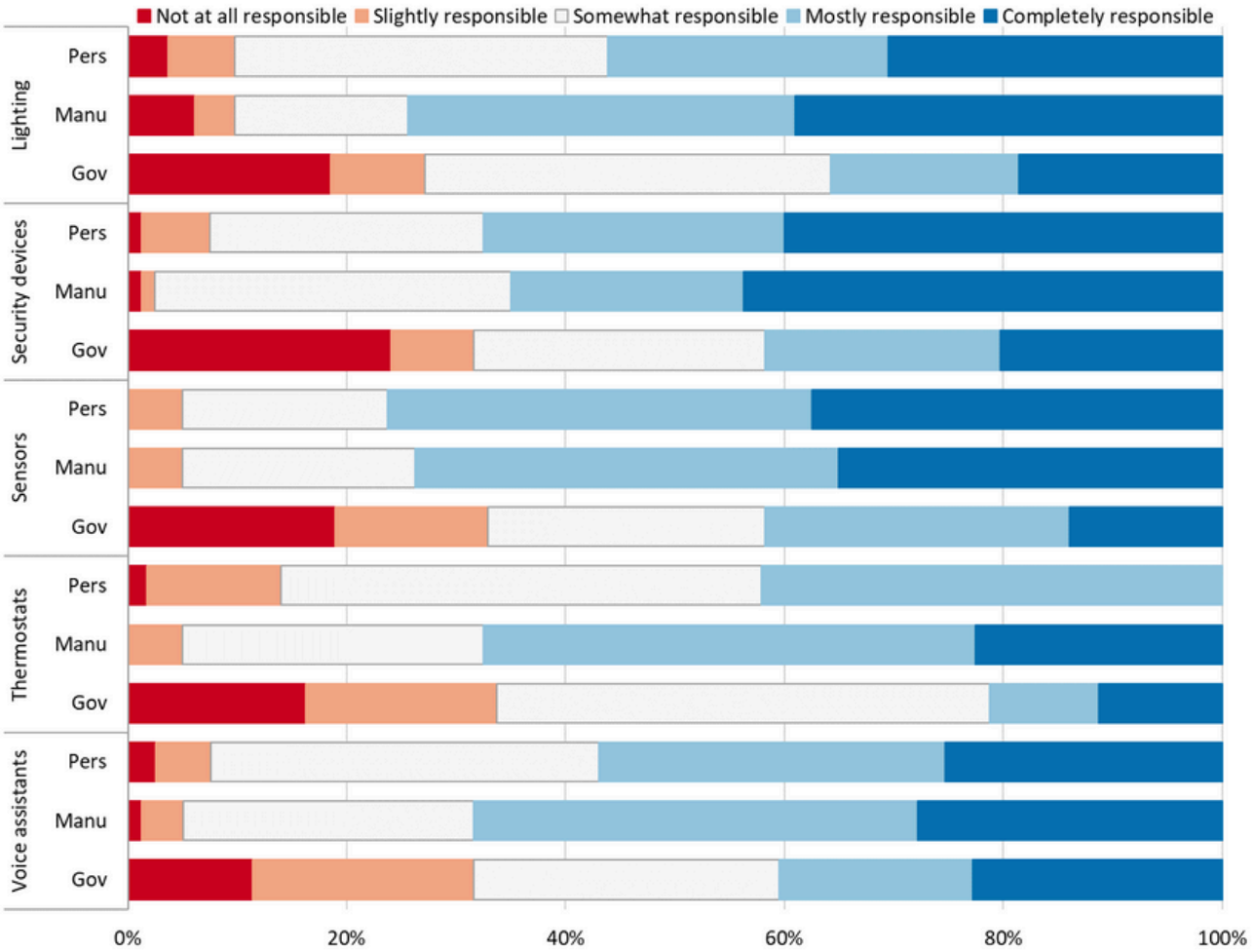


Figure 24. Participants' ratings of **ideal security** responsibility.
Pers = Personal responsibility
Manu = Manufacturer responsibility
Gov = Government responsibility

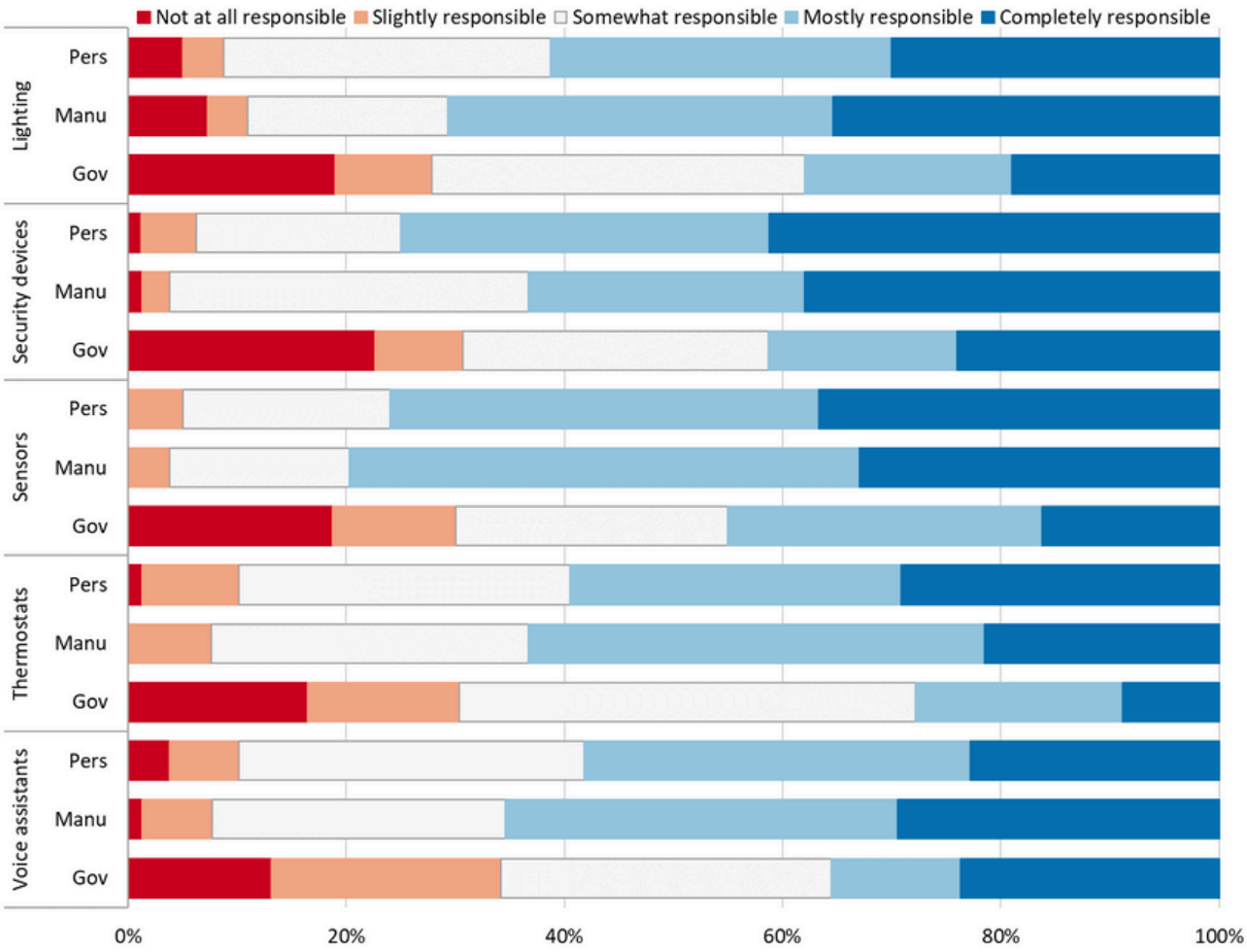


Figure 25. Participants' ratings of **ideal privacy** responsibility.
Pers = Personal responsibility
Manu = Manufacturer responsibility
Gov = Government responsibility

Almost all participants indicated that, ideally, manufacturers should be mostly or completely responsible for security, ranging from 65% (security devices) to 75% (lighting). Between 63% (security devices and thermostats) and 78% (sensors) thought manufacturers ideally should be at least somewhat responsible for device privacy.

Between 21% (thermostats) and 42% (security devices and sensors) thought the government ideally should be mostly or completely responsible for smart home **security**. For **privacy**, between 28% (thermostats) and 45% (sensors) thought the government ideally should be mostly/completely responsible.

Comparing ratings for current and ideal **security** responsibility (Fig. 26):

- participants with ***thermostats*** believed they should ideally take on more personal responsibility than they currently have,
- participants in ***all device categories*** thought manufacturers should ideally take on more responsibility than they currently have, and
- participants with ***sensors*** and ***voice assistants*** thought the government should ideally take on more responsibility than it currently has.

Comparing ratings for current and ideal **privacy** responsibility (Fig. 27):

- participants with ***lighting***, ***sensors***, and ***thermostats*** thought that manufacturers should ideally take on more responsibility than they currently have and
- participants with ***security devices*** and ***voice assistants*** thought the government should ideally take on more responsibility than it currently has.

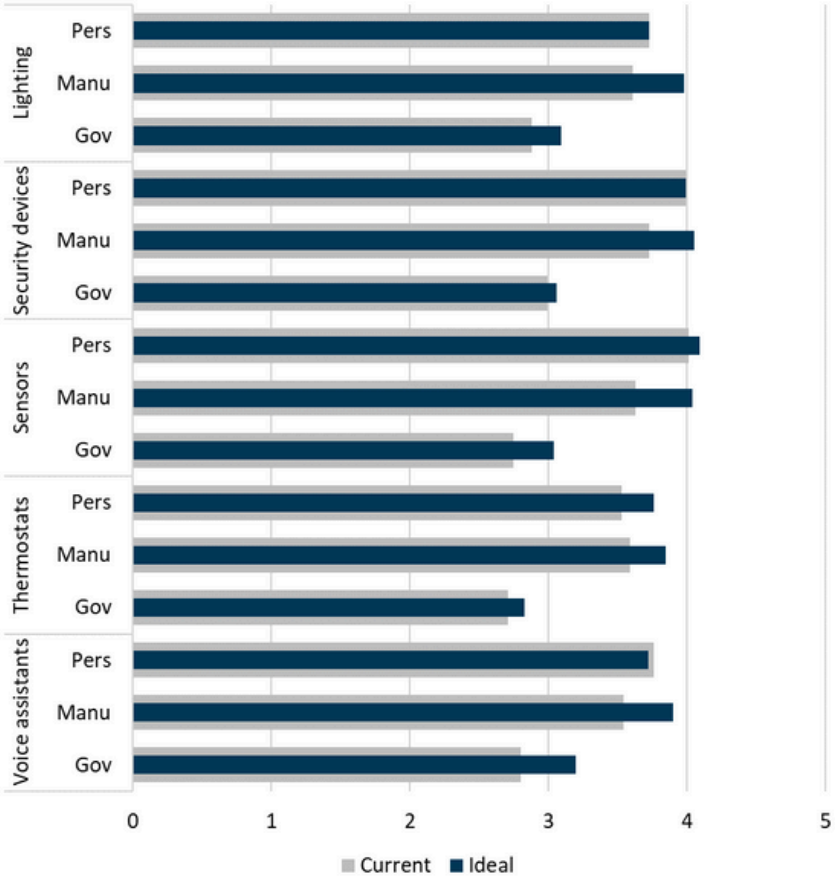


Figure 26. Mean (average) ratings of current vs. ideal **security** responsibility by device category. Ratings were on a 5-point scale ranging from Not at all responsible (1) to Completely Responsible (5).

Pers = Personal responsibility
Manu = Manufacturer responsibility
Gov = Government responsibility

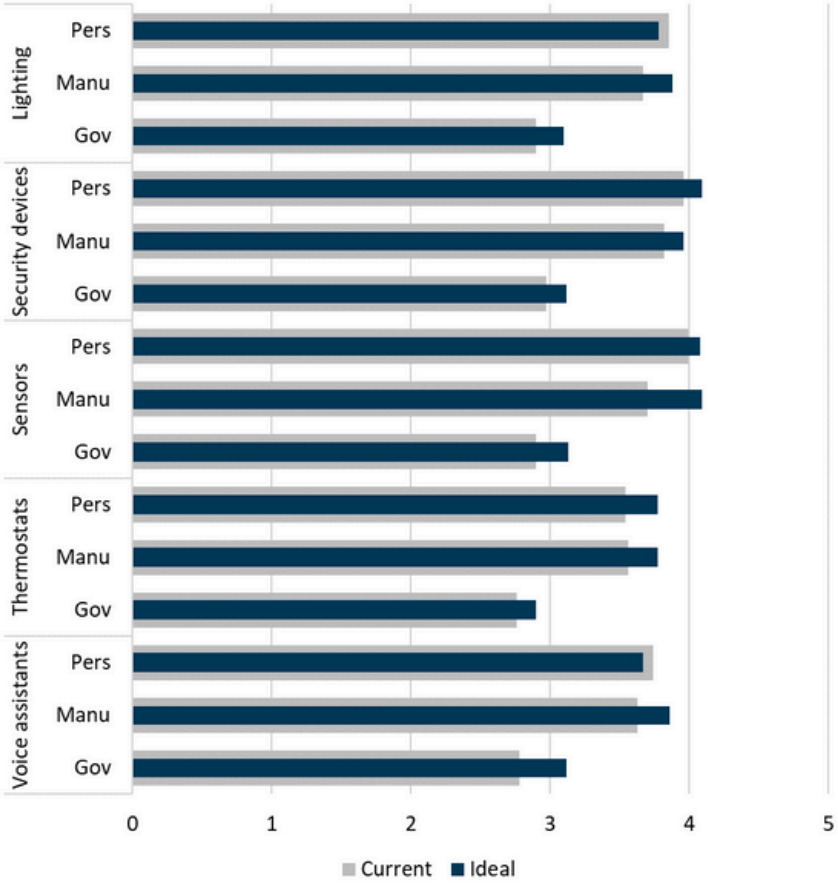


Figure 27. Mean (average) ratings of current vs. ideal **privacy** responsibility by device category. Ratings were on a 5-point scale ranging from Not at all responsible (1) to Completely Responsible (5).

Pers = Personal responsibility
Manu = Manufacturer responsibility
Gov = Government responsibility

INFORMATION SOURCES

To gain insight into sources and potential influence of smart home security and privacy information, we asked participants about:

- their current and preferred smart home security and privacy information sources
- the likelihood of smart home security and privacy information informing their future device purchases
- the likelihood of them acting on smart home security and privacy information
- trust of security and privacy ratings/labels from different sources

Current sources of smart home security and privacy information did not always align with preferred sources.

Participants selected *current* sources of smart home security and privacy information, then selected the sources from which they would *prefer* to receive information (Fig. 28).

Participants most often received information from manufacturer's website (46%), family or friends (34%), and the product package (25%). Source preferences somewhat differed. Participants most preferred to receive information from the manufacturer's website (49%), the product package (28%), an online retailer website (23%), and family or friends (23%). Few received or preferred to receive information at work.

Participants preferred to receive **less** smart home security and privacy information than they currently do from:

- social media
- family or friends

Participants preferred to receive **more** information from:

- device privacy policy or user agreement
- retail outlet shelf display
- security vulnerability repositories
- videos, webinars, or online training

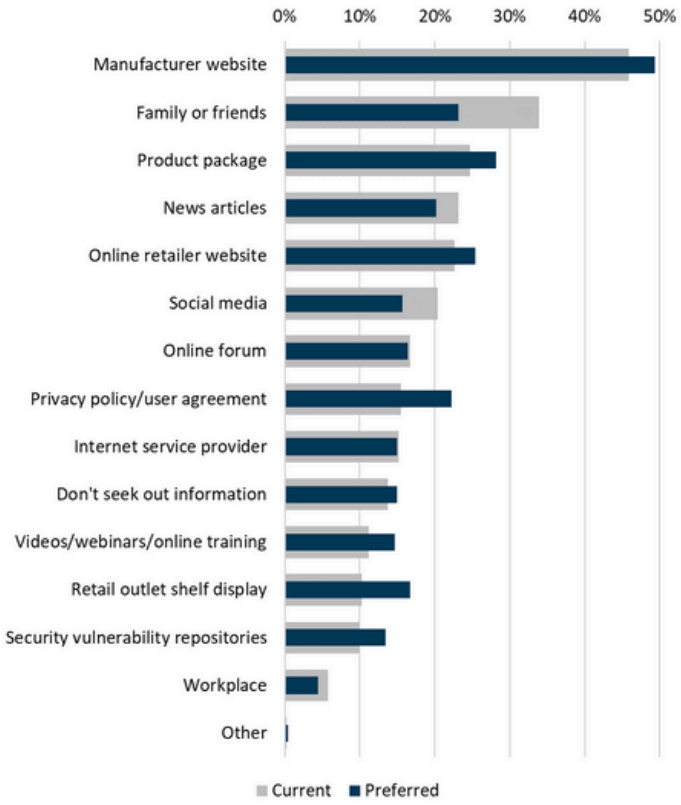


Figure 28. Percentages of participants selecting current and preferred sources of smart home security and privacy information

Most participants indicated that smart home security and privacy information would likely inform their future purchases.

Participants rated the likelihood that the following types of information might inform their future smart home purchases:

- smart home device security and privacy risks
- the device manufacturer's data practices
- device security features and options
- device privacy features and options
- whether the product meets a minimum security or privacy baseline

Over two-thirds of participants said that each type of information would likely or very likely inform their future purchases, ranging from 67% for information on risks and data practices to 71% for information on security features and options (Fig. 29).

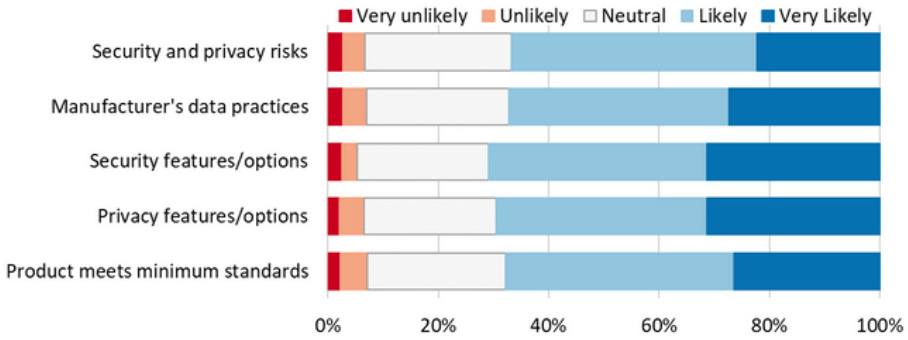


Figure 29. Participants' ratings of how likely they would be to use smart home security and privacy information to inform future purchases

Participants with ***thermostats*** were less likely to use security and privacy risk information to inform their future purchases compared to those with ***sensors***.

Participants were generally willing to act on smart home security and privacy information to protect their devices.

Participants rated the likelihood that they would act on the following types of information:

- information on how to better secure their smart home devices
- information on how to better secure their home network
- information on how to better protect their privacy when using their smart home devices

Over two-thirds of participants said that they would be likely or very likely to act on each type of information, ranging from 69% for information on how to better secure their devices and home network to 71% for information on how to better protect their privacy (Fig. 30).

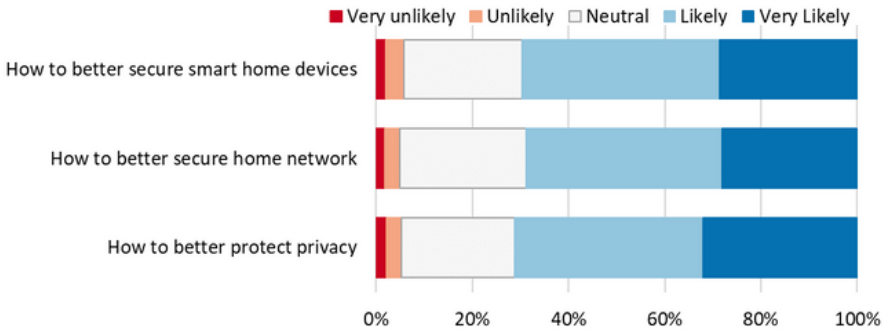


Figure 30. Participants' ratings of how likely they would be to act on smart home security and privacy information

Participants would be most trusting of security and privacy labels provided by the manufacturer or not-for-profit organizations.

Participants rated the level of trust they would have of a smart home device security or privacy rating or label if provided by the following entities on a 5-point scale ranging from very distrusting to very trusting:

- the U.S. Government
- the device manufacturer
- a not-for-profit organization
- a for-profit organization (other than the manufacturer)
- a smart home device retailer

Participants indicated that they would be most trusting (trusting or very trusting) of non-profit organizations or device manufacturers (51%) and least trusting of for-profit organizations (35% trusting/very trusting)and the U.S. Government (33% trusting/very trusting) (Fig. 31).

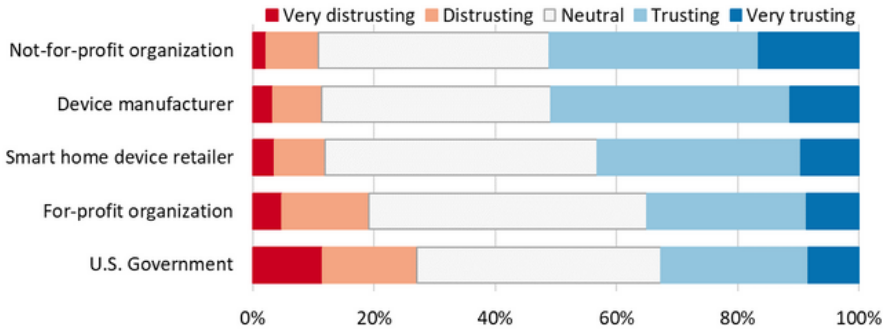


Figure 31. Participants' levels of trust of smart home security and privacy ratings/labels provided by different entities

Participants with ***thermostats*** were less likely to trust government labels compared to those with ***security devices***.

Participants with ***voice assistants*** were:

- less likely to trust labels from device manufacturers compared to participants with ***sensors*** and
- less likely to trust labels from retailers compared to those with ***security devices*** and ***sensors***.

Participants were less trusting of ***government*** labels as compared to labels that would come from ***all other types of organizations***.

Participants were less trusting of labels from ***retailers*** than labels from ***manufacturers*** and ***not-for-profit organizations***.

Participants were less trusting of labels from ***for-profit organizations*** than labels from ***manufacturers*** and ***not-for-profit organizations***.

Labels from ***for-profit organizations*** would be less trusted than labels from ***retailers*** ($z = -3.94$).

TAKEAWAYS

Based on the study results, we summarize device-specific takeaways and offer suggestions for how to improve consumer smart home education materials.

Per-Device Takeaways

We summarize high-level takeaways for each of the five smart home device categories of interest.

We observed a lack of trust of manufacturers and acknowledgement that smart **lighting** devices can be hacked. Participants also believed these devices do not provide enough configurable security and privacy options.

We found that, despite the video capabilities of some **security devices**, participants generally believe these to be secure and privacy-protecting by default and are more likely to trust the manufacturers. Yet, participants still accept more personal responsibility and take more actions on their own.

Participants generally believe **sensors** to be secure and privacy-protecting and are more satisfied with the actions they take.

Participants take fewer protective actions for **thermostats**, perhaps because they believe these are not likely to be hacked. They also tend to take on less personal responsibility of their devices but admit they should take on more.

Participants expressed unease with **voice assistants**, believing those to be less secure, having less understanding of security risks, and feeling less confident about their ability to protect these devices.

Tailoring Smart Home User Education

Based on the study results, we provide suggestions for tailoring smart home security and privacy education and awareness to reach and engage the U.S. smart home consumer population. These suggestions are targeted at stakeholders involved in communicating this information, including, but not limited to, device manufacturers, consumer advocacy groups, government agencies, standards bodies, and IoT label administrators, as well as researchers working in this space.

Emphasize that all types of devices may be at risk. To address potential misconceptions that some device categories (e.g., thermostats) require less intervention or vigilance, consumer education organizations and manufacturers could tailor device-specific materials that communicate 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 emphasize that compromise of "undervalued" devices with simple functionality (like sensors or thermostats) might lead to compromise of other, higher-value devices on the home network. Moreover, since security product labels (like the US Cyber Trust Mark [FCC 2024]) 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.

Clearly communicate security and privacy mechanisms. Manufacturer sources were most currently consulted and preferred. However, given the dearth of smart home security and privacy information available from manufacturers [NIST 2019], there is room for improvement. To address the consumers who have doubts about whether security and privacy options are available, manufacturers could utilize their own web presence to clearly communicate the security and privacy features included in the products, what risks these address, and what options are user-configurable and recommended. Product labels could provide a way for consumers to quickly find information about security and privacy features or, at a minimum, provide some assurance that a baseline has been met. In the case of a labeling program, a central repository of labeled products could provide links to manufacturer resources.

Encourage user action. Participants largely implemented simplistic mitigations, with more effective mitigations (like home network mitigations) being rarely employed. Yet, they still expressed some level of concern about the security and privacy of their devices. To help alleviate concerns and facilitate action, information providers could be clear about the responsibilities of consumers in protecting their devices and the information collected by devices. This is especially important in a product label scenario in which consumers still have responsibilities beyond the security and privacy features already included in a product. Resources should be easy-to-understand and include achievable steps to take action, especially for more advanced mitigations. Most

importantly, information sources should address common misconceptions that hinder people's motivation to take action, for example, not believing they will be targeted, not understanding risks, or thinking that labeled products are secure [NIST 2022][STANTON 2016][TABASSUM 2019][ZENG 2019].

Target multiple communication channels. Participants preferred to receive smart home security and privacy information in a variety of ways. Therefore, ensure that awareness and education campaigns distribute information via different channels, focusing specifically on manufacturer resources (e.g., websites, user agreements), retailer communications (e.g., online site, store shelves), and the smart home product package. Further, few participants indicated they receive information about smart home security and privacy from the workplace, perhaps highlighting a missed opportunity. There is an emerging trend of training programs creating a work-home connection by providing information on topics relevant to employees in their private lives [HANEY 2022]. Establishing this connection can help promote good security behavior habits regardless of context. In this vein, organizations could include smart home security and privacy information in their awareness efforts, perhaps drawing on already-created resources (e.g., tips from National Cybersecurity Alliance [NCA 2022]).

REFERENCES

[BUCHANAN 2018] Buchanan, E.M., & Scofield, J.E. (2018). Methods to detect low quality data and its implication for psychological research. *Behavior Research Methods* 50(6), 2586-2596.

[BUDIU 2018] Budiu, R. (2018). Between-Subjects vs. Within-Subjects Study Design. https://www.nngroup.com/articles/between-within-subjects/

[CHARNESS 2012] Charness, G., Gneezy, U., & Kuhn, M.A. (2012). Experimental methods: Between-subject and within-subject design. *Journal of Economic Behavior & Organization* 81(1), 1-8.

[COHEN 1992] Cohen, J. (1992). A Power Primer. *Psychological Bulletin* 112(1).

[CSDE 2019] Council to Secure the Digital Economy (2019). The C2 Consensus on IoT Security Baseline Capabilities. https://securingdigitaleconomy.org/projects/c2-consensus/

[DOGRUEL 2019] Dogruel, L., & Joeckel, S. (2019). 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.

[EMAMI-NAEINI 2021] Emami-Naeini, P., Dheenadhayalan, J., Agarwal, Y., & Cranor, L. F. (2021, May). 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. 519-536). IEEE.

[ETSI 2020] ETSI Technical Committee Cyber Security (2020). 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

[EU 2019] European Union Agency for Cybersecurity (2019). Good Practices for Security of {IoT} - Secure Software Development Lifecycle. https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1

[FASSL 2021] Fassl, M., Neumayr, M., Schedler, O., & Krombholz, K. (2021, October). Transferring update behavior from smartphones to smart consumer devices. In European Symposium on Research in Computer Security (pp. 357-383). Cham: Springer International Publishing.

[FAUL 2009] Faul, F., Erdfeder, E., Buchner, A., & Lang, A. (2009). Statistical power analyses using G* Power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods* 41(4), 1149-1160.

[FCC 2024] Federal Communications Commission (2024). FCC Creates voluntary cybersecurity labeling program for smart products. https://docs.fcc.gov/public/attachments/DOC-401201A1.pdf

[HANEY 2020] Haney, J. M., Furman, S. M., & Acar, Y. (2020). Smart home security and privacy mitigations: Consumer perceptions, practices, and challenges. In HCI for Cybersecurity, Privacy and Trust: Second International Conference, HCI-CPT 2020, Held as Part of the 22nd HCI International Conference, HCII 2020, Copenhagen, Denmark, July 19–24, 2020, Proceedings 22 (pp. 393-411). Springer International Publishing.

[HANEY 2021] Haney, J., Acar, Y., & Furman, S. (2021). "It's the Company, the Government, You and I": User Perceptions of Responsibility for Smart Home Privacy and Security. In 30th USENIX Security Symposium (USENIX Security 21) (pp. 411-428).

[HANEY 2022] Haney, J., Jacobs, J., & Furman, S. (2022) NISTIR 8420A Approaches and challenges of federal cybersecurity awareness programs. https://www.nist.gov/publications/approaches-and-challenges-federal-cybersecurity-awareness-programs

[HANEY 2023] Haney, J. M., & Furman, S. M. (2023, May). User perceptions and experiences with smart home updates. In 2023 IEEE Symposium on Security and Privacy (SP) (pp. 2867-2884). IEEE.

[HARRIS 2019] Harris Interactive (2019). 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.

[HERATH 2009] Herath, T., & Rao, H.R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems* 47(2), 154-165.

[IOTSF 2021] IoT Security Foundation (2021). IoT Security Assurance Framework. https://iotsecurityfoundation.org/wp-content/uploads/2021/11/IoTSF-IoT-Security-Assurance-Framework-Release-3.0-Nov-2021-1.pdf

[KIM 2017] Kim, H. (2017). Statistical notes for clinical researchers: Chi-squared test and Fisher's exact test. *Restorative Dentistry & Endodontics* 42(2), 152-155.

[LAU 2018] Lau, J., Zimmerman, B., & Schaub, F. (2018). Alexa, are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. Proceedings of the ACM on human-computer interaction, 2(CSCW), 1-31.

[LEWIS 1997] Lewis, C., Wharton, C. (1997). Cognitive walkthroughs. In M. G. Helander, T. K. Landauer, P. V. Prabhu (Eds.), *Handbook of Human-Computer Interaction* (pp. 717-732). North-Holland.

[MALHOTRA 2008] Malhotra, N. (2008). Completion time and response order effects in web surveys. *Public Opinion Quarterly* 72(5), 914-934.

[MALKIN 2019] Malkin, N., Deatrick, J., Tong, A., Wijesekera, P., Egelman, S., & Wagner, D. (2019). Privacy attitudes of smart speaker users. Proceedings on Privacy Enhancing Technologies, 2019(4).

[MANGIAFICO 2023] Mangiafico, S.S. (2023), Summary and Analysis of Extension Program Evaluation in R, version 1.20.05. https://rcompanion.org/handbook/

[NCA 2022] National Cybersecurity Alliance (2022). Secure Your Home. https://www.staysafeonline.org/articles/secure-your-home

[NIST 2022] National Institute of Standards and Technology (2022). Recommended criteria for cybersecurity labeling for consumer internet of things (IoT) products. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf

[NPD 2021] NPD Group (2021). 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/

[NURSE 2022] Nurse, J.R.C., Karppinen, I., Milward, J., & Varughese, J. (2022). Oh behave! The annual cybersecurity attitudes and behaviors report. https://staysafeonline.org/online-safety-privacy-basics/oh-behave/

[PALLANT 2020] Pallant, J. (2020). *SPSS survival manual: A step by step guide to data analysis using IBM SPSS*. McGraw-Hill Education.

[PARKS ASSOCIATES 2024] Parks Associates (2024). Survey: 18% US homes have 6 or more smart devices. https://www.parksassociates.com/blogs/in-the-news/survey-18-us-homes-have-6-or-more-smart-devices

[POULTON 1973] Poulton, E.C. (1973). Unwanted range effects from using within-subject experimental designs. *Psychological Bulletin* 80(2), 113-121.

[POWERS 1973] Powers, W.T. (1973). *Behavior: The Control of Perception*. Aldine.

[REDMILES 2016] Redmiles, E.M., Kross, S., & Mazurek, M.L. (2016). How I learned to be secure: a census-representative survey of security advice sources and behavior. In 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 666-677).

[SERDAR 2021] Serdar, C.C., Cihan, M., Yucel, D., & Serdar, M.A. (2021). Sample size, power and effect size revisited: simplified and practical approaches in pre-clinical, clinical and laboratory studies. *Biochemia Medica* 31(1), 27-53.

[STANTON 2016] Stanton, B., Theofanos, M.F., Prettyman, S.S., & Furman, S. (2016). Security fatigue. *IT Professional* 18(5), 26-32.

[STATISTA 2020] Statista (2020). Smart Home penetration rate forecast for selected countries 2020. https://www.statista.com/forecasts/483757/penetration-rate-of-smart-homes-for-selected-countries

[SULLIVAN 2012] Sullivan, G.M., & Feinn, R. (2012). Using effect size—or why the P value is not enough. Journal of Graduate Medical Education 4(3), 279-282.

[TABASSUM 2019] Tabassum, M., Kosinski, T., & Lipford, H. R. (2019). " I don't own the data": End User Perceptions of Smart Home Device Data Practices and Risks. In Fifteenth symposium on usable privacy and security (SOUPS 2019) (pp. 435-450).

[US CENSUS 2022] United States Census Bureau (2022). Basic Monthly CPS. https://www.census.gov/data/datasets/time-series/demo/cps/cps-basic.html

[ZENG 2017] Zeng, E., Mare, S., & Roesner, F. (2017). End user security and privacy concerns with smart homes. In thirteenth symposium on usable privacy and security (SOUPS 2017) (pp. 65-80).

[ZHENG 2018] Zheng, S., Apthorpe, N., Chetty, M., & Feamster, N. (2018). User perceptions of smart home IoT privacy. Proceedings of the ACM on human-computer interaction, 2(CSCW), 1-20.

TECHNICAL APPENDIX

This appendix contains additional details about the study for those who are interested, including:

- **Detailed Methodology: study design, participant recruitment, data collection, data analysis, ethics, and study limitations**
- **Additional Demographics: more details about the survey participants**
- **Statistical Results: detailed statistical analysis data**
- **Survey Instrument: survey questions and answer options**

DETAILED METHODOLOGY

Study Design

We opted to conduct an anonymous, online survey to answer our research questions. The survey format allowed us to efficiently sample a large number of smart home users while leveraging prior qualitative work to inform the development of survey questions and response options

Survey Topics

We opted to conduct an anonymous, online survey to answer our research questions. The survey format allowed us to efficiently sample a large number of smart home users while leveraging prior qualitative work to inform the development of survey questions and response options

We developed the survey based on our research questions and findings of prior user-focused research on smart home security and privacy. We report results from the final survey addressing the following topics aligned with our research questions and informed by the cited literature.

RQ1: How do users' perceptions about the security and privacy of their smart home devices differ across device categories?

- perceptions about device security/privacy [HANEY 2023]
- level of security and privacy concern [HANEY 2023]
- reasons for lack of concern or using smart home devices despite concerns [HANEY 2020][HANEY 2021][TABASSUM 2019][ZHENG 2018]

RQ2: How do users' security and privacy actions and perceptions about taking action differ across device categories?

- any security and privacy actions participants took to protect their devices and how effective participants believed those actions to be [HANEY 2020][TABASSUM 2019][ZENG 2017][ZHENG 2018]
- perceived ability to protect devices [HANEY 2021][LAU 2018]
- perceived barriers to taking action [HANEY 2020][TABASSUM 2019][ZHENG 2018]

RQ3: How do users' perceptions of who is responsible for smart home security and privacy differ across device categories?

- perceptions about how much responsibility participants, device manufacturers, and the U.S. Government have for smart home security and privacy [HANEY 2021]

RQ4: From which information sources do users currently and prefer to receive smart home security and privacy information?

- current and preferred sources for information on smart home security and privacy [HARRIS 2019][REDMILES 2016]

RQ5: What is the likelihood that security and privacy information will influence users' smart home purchases and actions?

- likelihood of security and privacy information informing future smart home purchases [EMAMI-NAEINI 2021]
- likelihood that information would influence security and privacy actions [EMAMI-NAEINI 2021]
- trust of security and privacy ratings provided by different entities

The survey focused on five smart home device categories: smart lighting, smart security devices, smart sensors, smart thermostats, and voice assistants/smart speakers. We selected these categories as a basis for comparison with prior NIST studies that specified that participants had to be active users of devices in those same categories [HANEY 2021][HANEY 2023]. These were also among the most popular in the U.S. at the time of the survey data collection [NPD 2021][STATISTA 2020] and represented different degrees of sophistication and potential security implications.

Between-Subjects Design

Our study was, in part, inspired by a prior within-subjects NIST smart home survey in which participants provided ratings for each of the device categories they used [HANEY 2023]. However, we opted for a between-subjects design to mitigate some of the 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 demand effects (participants interpreting experimenter's intentions based on the comparisons), range effects (in which responses are potentially influenced by the perceived range of presented items and a central tendency), and potential ordering effects based on how the compared items are presented [CHARNESS 2012][POULTON 1973].

Conversely, a between-subjects survey minimizes the transfer across conditions and is shorter in duration, potentially providing a higher likelihood that respondents will complete the survey [BUDIU 2018]. In addition, for scenarios in which an individual is not likely to do a comparison when making decisions in real life -- which is the case in our study context -- between-subjects may provide more external validity [CHARNESS 2012]. For example, users likely do not compare the security attributes of a voice assistant to those of a smart light bulb when making decisions about or taking action on their smart light bulb.

Survey Review and Refinement

After crafting an initial draft of the survey, we conducted three rounds of reviews to ensure survey content and construct validity, refining the survey instrument after each round. In the first round, an IoT security expert reviewed the survey for technical accuracy and completeness and alignment with research questions. In a second round of review, two survey experts reviewed the survey with a focus on clarity, use of plain language, and alignment of response options to questions. Finally, as a further clarity check, we conducted cognitive walkthroughs with two individuals representative of our target population to gather feedback on how respondents might interpret and answer the survey questions [LEWIS 1997]. As a result of these reviews, we made minor edits to improve the instrument.

The final survey is included later in this appendix: **Survey Instrument**.

Sample Size Estimation

Per our between-subjects design, participants answered survey questions based on only one device category. Using G*Power [FAUL 2009], we determined a minimum sample size of 305 needed for a Kruskal Wallis H Test (non-parametric ANOVA) with five independent groups (device categories) to achieve a power of 0.95, a medium effect size, and $\alpha = 0.05$, which are standard thresholds used in statistical analysis [SERDAR 2021]. Also using G*Power, we confirmed that this sample size was more than sufficient for the sample of 57 required for a Wilcoxon signed-rank test (matched pairs) with a power of 0.95, a medium effect size, and $\alpha = 0.05$. To meet and exceed the minimum sample size, we aimed for 400 participants, with 80 participants for each device category.

Participant Recruitment

We recruited survey participants using the Prodege opt-in consumer research panel. The panel allowed for granular sampling and recruitment that could be dynamically adjusted to fill gaps in desired demographics as the survey timeframe progressed and included a smart home ownership attribute that facilitated targeted recruitment. To be eligible for the survey, prospective participants had to be adults (18+ years old) living in the U.S. and active users of smart home devices in at least one of the five device categories of interest.

While our goal was not to have a sample that was fully representative of the U.S. population, we wished to recruit participants from various demographic groups to sample the full range of U.S. smart home users. Thus, we developed soft quotas (optional targets) for various demographics and U.S. region based on data published by the U.S. Census Bureau's Current Population Survey (CPS) Basic Monthly survey [US CENSUS 2022].

Data Collection

We fielded the online survey for two weeks in February 2022, with survey invitations sent out incrementally to Prodege panel members.

Prospective participants completed a screening question asking them to indicate the categories of any smart home devices they actively used. If they were users of a device in at least one category of interest, we randomly assigned them to complete the survey based on one of their selected categories for which the participant quota had not yet been met. For example, if a participant indicated that they owned smart home devices in the voice assistant, thermostat, and lighting categories, but the quota for voice assistant responses had already been met, they might be randomly asked to complete the survey based on their lighting device. If the participant indicated using only device categories with filled quotas, they were not invited to complete the survey.

While 405 participants completed the survey, four responses were removed due to failure to meet the criteria of being active users or a survey completion time more than 1.5 standard deviations below the average completion time, as recommended by survey methodologists [BUCHANAN 2018] [MALHOTRA 2008]. A total of 401 responses were included in the final data set: 79 for voice assistants, 80 for thermostats, 80 for security devices, 80 for sensors, and 82 for lighting. Note that because of timing issues in the survey platform with respect to notification that a category quota had been met, it was possible for a category to have over 80 participants, as was the case for lighting.

Data Analysis

We first calculated descriptive statistics to summarize response frequencies and inferential statistics at a significance level of $\alpha = 0.05$ using the statistical analysis software Stata.

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 correction to account for multiple comparisons. Significant results are reported with the *z*-statistic.

We used ANOVA and post-hoc pairwise comparisons with a Holm-Bonferroni correction to explore differences across categories for the 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 used 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.

We also investigated significant differences between related question responses. We performed the Wilcoxon matched-pairs signed rank test to compare ordinal response questions, reporting statistically significant results with the *z*-statistic. Specifically, we used this statistical test to determine if there were significant differences between participants' ratings of the likelihood of using security and privacy risk information to inform their purchase decisions versus the likelihood of using information on data practices.

We performed McNemar's test (a type of paired Chi-square test) to look for significant differences between pairs of questions with dichotomous categorical variables. For example, we used this test to compare participants' current use of online information sources (checked or unchecked) and their preferred use of online sources (checked or unchecked). We report significant McNemar's test results with χ^2 (degrees of freedom = 1 for all tests).

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 [SULLIVAN 2012]. See Table 2 for the effect sizes for each statistical test.

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

Index	Test	Small	Medium	Large
Independent groups				
Cohen's d (d) [COHEN 1992]	Mann-Whitney U Test ANOVA	0.20	0.50	0.80
Cramer's V (V) [KIM 2017]	Chi square	0.10	0.30	0.50
Matched data				
Effect size (r) [PALLANT 2011]	Wilcoxon signed-rank test	0.10	0.30	0.50
Odds ratio (OR) [MANGIAFICO 2023]	McNemar's test	1.22 (0.538, 0.82]	1.86 (0.333, 0.538]	3.00 (∞ , 0.333]

Ethics

The NIST Research Protections Office determined that the study protocol met the criteria for "exempt human subjects research" as defined in 15 CFR 27, the Common Rule for the Protection of Human Subjects.

On the first survey screen, we provided participants with information describing the study purpose, procedure, and data protection measures. Survey data were anonymous and participants had the option to skip any survey question. Participants received a $12.50 gift card for an average completion time of 13 minutes, which was well above minimum wage in the U.S. ($7.25 - $16.10 per hour).

Study Limitations

The study has several limitations. Self-report data may be subject to recall bias, as in the case of reported information sources and actions. Furthermore, participants' perceptions of the likelihood of security and privacy information informing their future purchase decisions and obstacles to actions may not reflect the actions they ultimately take. However, perceptions do influence behaviors [HERATH 2009][POWERS 1973].

We sampled participants in the U.S., who may differ in their attitudes and actions from smart home consumers in other countries [DOGRUEL 2019][NURSE 2022]. We also cannot generalize our results to users of other categories of devices not included in our recruitment criteria. Moreover, there may be other influences on consumer perceptions not investigated here, which we leave to future work.

Finally, we looked at both security and privacy aspects, yet people may conflate these concepts [ZHENG 2018]. To counter this, we provided definitions in the survey to distinguish the two terms. These definitions were adapted from a user-focused survey on smart home updates [HANEY 2023]. In that survey, participants did distinguish between the two concepts when expressing their perceptions of device security and privacy. In our survey, we also found some differences in predictors for paired questions on security and privacy.

ADDITIONAL DEMOGRAPHICS

Table 3: Additional demographic data of 401 survey participants

Variable	Groups	Number	Percentage
U.S. Region	South	155	38.7%
	West	88	21.9%
	Midwest	79	19.7%
	Northeast	72	18.0%
	No answer	7	1.7%
Home ownership	Own	260	64.8%
	Rent	115	28.7%
	Other	13	3.2%
	No answer	13	3.2%
Urbanicity	Suburban	225	56.1%
	Urban	102	25.4%
	Rural	67	16.7%
	No answer	7	1.7%
Employment status	Employed full-time	183	45.6%
	Retired	80	20.0%
	Not employed	61	15.2%
	Employed part-time	41	10.2%
	Full-time student	30	7.5%
	No answer	6	1.5%
IT experience	No	343	85.5%
	Yes	53	13.2%
	No answer	5	1.2%

STATISTICAL RESULTS

Inferential statistics for the call-out boxes in the main report are included in this section.

For each statistically significant result, we report the heading under which it appeared, the statistical test, and the plain language statement, which includes the test statistic, an indicator of the significance level, and the effect size.

Significance levels:
* $p < 0.05$
** $p \leq 0.01$
*** $p \leq 0.001$

Participants rated voice assistants as least secure and privacy protecting.

Statistical test: Dunn's test with Holm-Bonferroni corrections

Participants believed their voice assistants were significantly less secure and privacy-respecting than all other device categories (see Table 4).

Table 4: Statistical results for security and privacy ratings

Pairwise Comparison	Security	Privacy
lighting – voice assistants	z = 3.15***, d = 0.46	z = 2.74*, d = 0.45
security devices – voice assistants	z = 5.51***, d = 0.87	z = 4.55***, d = 0.72
sensors – voice assistants	z = 4.30***, d = 0.61	z = 3.45**, d = 0.52
thermostats – voice assistants	z = 3.17***, d = 0.56	z = 2.85*, d = 0.55

Participants generally believed they understood the security and privacy risks of their smart home devices.

Statistical test: Dunn's test with Holm-Bonferroni corrections

Participants thought they had much less understanding of security risks for voice assistants than they did for security devices (z = -3.59**, d = 0.56).

Participants had varying beliefs about security and privacy which, in part, explained their levels of concern.

Statistical test: Chi-square test of independence with 1 degree of freedom and Holm-Bonferroni corrections

Participants with thermostats were more likely to believe that the chances of their devices being hacked were low compared to participants with smart lighting (χ^2= 10.66***, V = 0.26) and voice assistants (χ^2= 10.84***, V = 0.26).

Participants with sensors more often thought that their actions alleviated their concerns than those with thermostats (χ^2= 9.00**, V = 0.24).

Participants with smart security devices more often said that they trusted the manufacturer to protect their privacy as compared to participants with lighting (χ^2= 12.08***, V = 0.27) and voice assistants (χ^2= 14.14***, V = 0.30).

Participants took a variety of security and privacy actions, with most being simplistic.

Statistical test: Chi-square test of independence with 1 degree of freedom and Holm-Bonferroni corrections

Participants with security devices more often set a password or PIN compared to participants with smart lighting (χ^2= 11.99***, V = 0.27)or voice assistants (χ^2= 10.57***, V = 0.36).

Participants with voice assistants less often set up or changed security or privacy options compared to those with devices in all other categories: lighting (χ^2= 16.54***, V = 0.32), security devices (χ^2= 18.27***, V = 0.34), sensors (χ^2= 15.81***, V = 0.32), thermostats (χ^2= 12.26***, V = 0.28).

Participants with thermostats:

- less often take care not to place their devices in sensitive or private areas of the home compared to participants with security devices (χ^2= 12.97***, V = 0.28) and voice assistants (χ^2= 8.33**, V = 0.23) and
- less often said they were careful about what they say or do near their devices than participants with devices in all other categories: lighting (χ^2= 8.19**, V = 0.22), security devices (χ^2= 20.20***, V = 0.36), sensors (χ^2= 10.67***, V = 0.26), voice assistants (χ^2= 18.00***, V = 0.34).

Participants took more actions for smart security devices.

Statistical test: ANOVA with Holm-Bonferroni corrections

Participants with security devices (3.0 actions on average) took significantly more actions as compared to those with smart lighting (2.2 actions on average) (t = 1.27**, d = 0.41), voice assistants (2.0 actions) (t = 3.46***, d=0.54), and thermostats (1.8 actions) (t = 3.96***, d = 0.60).

Participants felt less able to protect their voice assistants.

Statistical test: Dunn's test with Holm-Bonferroni corrections

Participants with voice assistants felt significantly:

- less able to protect device security compared to participants with smart security devices (z = -2.21**, d = 0.51) and
- less able to protect their privacy as compared to those with devices in all other categories: lighting (z = 3.51**, d = 0.56), security devices (z = -3.51**, d = 0.57), sensors (z = -4.04***, d = 0.62), thermostats (z = -2.83*, d = 0.49).

Participants expressed varied obstacles to taking action.

Statistical test: Chi-square test of independence with 1 degree of freedom and Holm-Bonferroni corrections

For security obstacles, participants with voice assistants indicated that nothing prevents them because they were satisfied with the actions they had already taken less often compared to those with thermostats (χ^2= 18.94***, V = 0.35).

For privacy, participants with thermostats:

- more often said that nothing prevents them because they were satisfied with the actions they had already taken, as compared to those with voice assistants (χ^2= 22.90***, V = 0.38), security devices (χ^2= 10.99***, V = 0.26), and smart lighting (χ^2= 9.41**, V = 0.24) and
- less often indicated that there are no options for setting their privacy preferences than participants with smart lighting (χ^2= 8.57**, V = 0.23).
-

For privacy, participants with sensors said that nothing prevents them because they were satisfied with the actions they had already taken, as compared to those with voice assistants (χ^2= 9.90**, V = 0.25).

Participants viewed current responsibility for smart home security and privacy as being shared.

Statistical test: Dunn's test with Holm-Bonferroni corrections

Participants assigned significantly less personal security responsibility for thermostats compared to security devices (z = -2.92*, d = 0.42) and sensors (z = -2.98*, d = 0.46).

Participants believed manufacturers and the government should take on more responsibility.

Statistical test: Wilcoxon signed rank test

Comparing ratings for current and ideal security responsibility (Fig. x):

- participants with thermostats believed they should ideally take on more personal responsibility than they currently have (z = 2.48*, r = 0.28);
- participants in all device categories thought manufacturers should ideally take on more responsibility than they currently have: lighting (z = 4.19***, r = 0.46), security devices (z = 3.85***, r = 0.43), sensors (z = 2.96**, r = 0.33), thermostats (z = 2.95**, r = 0.33), voice assistants (z = 3.38***, r = 0.38);
- participants with sensors (z = 2.82**, r = 0.32) and voice assistants (z = 3.0**, r = 0.34) thought the government should ideally take on more responsibility than it currently has.

Comparing ratings for current and ideal privacy responsibility (Fig. x):

- participants with lighting (z = 2.21*, r = 0.24), sensors (z = 3.12**, r = 0.35), and thermostats (z = 2.23*, r = 0.25)thought that manufacturers should ideally take on more responsibility than they currently have and
- participants with security devices (z = 2.43*, r = 0.28) and voice assistants (z = 2.82**, r = 0.32) thought the government should ideally take on more responsibility than it currently has.

Current sources of smart home security and privacy information did not always align with preferred sources.

Statistical test: McNemar's test

Participants preferred to receive less smart home security and privacy information than they currently do from:

- social media (chi2 = 5.92*, OR = 1.90)
- family or friends (chi2 = 24.65***, OR = 3.69)
-

Participants preferred to receive more information from:

- device privacy policy or user agreement (chi2 = 9.99**, OR = 0.46)
- retail outlet shelf display (chi2 = 9.94**, OR = 0.45)
- security vulnerability repositories (chi2 = 8.07**, OR = 0.46)
- videos, webinars, or online training (chi2 = 4.08*, OR = 0.55)

Most participants indicated that smart home security and privacy information would likely inform their future purchases.

Statistical test: Dunn's test with Holm-Bonferroni corrections

Participants with thermostats were less likely to use security and privacy risk information to inform their future purchases compared to those with sensors (z = -2.82*, d = 0.43).

Participants would be most trusting of security and privacy labels provided by the manufacturer or not-for-profit organizations.

Statistical test: Dunn's test with Holm-Bonferroni corrections

Participants with thermostats were less likely to trust government labels compared to those with security devices (z =-2.90*, d = 0.47).

Participants with voice assistants were:

- less likely to trust labels from device manufacturers compared to participants with sensors (z = -3.62**, d = 0.53) and
- less likely to trust labels from retailers compared to those with security devices (z = -3.4**, d = 0.61) and sensors (z = -4.25***, d = 0.63).

Participants would be most trusting of security and privacy labels provided by the manufacturer or not-for-profit organizations.

Statistical test: Wilcoxon signed rank test

Participants were less trusting of government labels as compared to labels that would come from all other types of organizations: manufacturers (z = -7.75***, r = 0.39), not-for-profit organizations (z = -8.35***, r = 0.42), for-profits (z = -2.88**, r = 0.14), and retailers (z = -6.21***, r = 0.31).

Participants were less trusting of labels from retailers than labels from manufacturers (z = 3.18**, r = 0.16) and not-for-profit organizations (z = 3.17**, r = 0.16).

Participants were less trusting of labels from for-profit organizations than labels from manufacturers (z = 5.69***, r = 0.29) and not-for-profit organizations (z = 6.49***, r = 0.33).

Labels from for-profit organizations would be less trusted than labels from retailers (z = -3.94***, r = 0.20).

SURVEY INSTRUMENT

The following is the subset of the survey reported in this document.

[redacted]

Smart Home Security and Privacy Survey

OMB #0693-0043 3/31/2022

This survey is being conducted on behalf of the National Institute of Standards and Technology (NIST), which, in part, works with industry and other agencies to develop information technology (IT) standards and cultivate trust in IT. For this effort, NIST is interested in users of smart home devices and their thoughts about the security and privacy of those devices. NIST has partnered with Fors Marsh Group (FMG), an independent research firm, to administer this survey and learn more about consumers' smart home security and privacy concerns, actions, information sources, and expectations. Your responses will assist NIST in improving standards for smart home devices.

Please know that nothing you share will be connected to your name. We are collecting this information strictly to inform our research, and all of your information will be kept confidential.

It is important that you know the following information before you decide to complete the survey:

- ***Purpose***: This study is being performed to understand consumers' smart home security and privacy concerns, actions, information sources, and expectations.
- ***Duration***: We anticipate that your participation in this research study will take approximately 20 minutes.
- ***Procedures and Activities***: You will complete an online survey regarding your security and privacy concerns, actions, and perceptions related to your smart home devices. Your survey response will be collected without any personal identifiers.
- ***Voluntary consent***: Taking part in this study is completely voluntary. You may decide to participate or not participate.
- ***Risks and Benefits***: This research is considered to be minimal risk. That means that the risks associated with this study are the same as what you face every day. You will not benefit directly by participating in the study. The long-term benefits of this study should be improved standards for the usability, security, and privacy of smart home devices.

We also have more detailed information available to you about this survey and your privacy. Select the additional pages you would like to read below, if any, before proceeding with the survey. [redacted]

☐ NIST Information Sheet

By continuing with the survey, you acknowledge that the following is true for you:

I understand the above description of the research and the risks and benefits associated with my participation as a research subject. I understand that by proceeding with this survey I agree to take part in this research and do so voluntarily.

If you have any technical issues while taking the survey, please email the help desk at NISTHomeSurvey@forsmarshgroup.com. If you have any questions regarding incentives, please contact [redacted]

Thank you for your time and participation! When you are ready to begin the survey, click Next.

Next »

A Federal agency may not conduct or sponsor, and a person is not required to respond to, nor shall a person be subject to a penalty for failure to comply with an information collection subject to the requirements of the Paperwork Reduction Act of 1995 unless the information collection has a currently valid OMB Control Number. The approved OMB Control Number for this information collection is 0693-0043. Without this approval, we could not conduct this survey. Public reporting for this information collection is estimated to be approximately 20 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the information collection. All responses to this information collection are voluntary. Send comments regarding this burden estimate or any other aspect of this information collection, including suggestions for reducing this burden to the National Institute of Standards and Technology at: Attn: Julie Haney, 100 Bureau Drive, Gaithersburg, MD 20899 or

Information Sheet:

Smart Home Security and Privacy Survey

Information Sheet for Study

Principal Investigator: Julie Haney, National Institute of Standards and Technology
Study Title: Smart Home Security and Privacy Survey
Study Site(s): Online survey is administered by Fors Marsh Group.

Key Information

This is a brief summary of key information to describe the research study you are being invited to participate in. You will find more detailed information explained later in this document.

- ***Purpose:*** This study is being performed to understand consumers' smart home security and privacy concerns, actions, information sources, and expectations.
- ***Duration:*** We anticipate that your participation in this research study will take approximately 20 minutes.
- ***Procedures and Activities:*** You will complete an online survey regarding your security and privacy concerns, actions, and perceptions related to your smart home devices. Your survey response will be collected without any personal identifiers.
- ***Voluntary consent:*** Taking part in this study is completely voluntary. You may decide to participate or not participate.
- ***Risks and Benefits:*** This research is considered to be minimal risk. That means that the risks associated with this study are the same as what you face every day. You will not benefit directly by participating in the study. The long-term benefits of this study should be improved standards for the usability, security, and privacy of smart home devices.

Introduction
You are being asked to take part in a research study. Research studies include only people who choose to take part. This document is called an information sheet and is for you to read carefully before you make your decision about participating in the study. Ask the researcher or study staff to discuss this information sheet with you. Please ask them to explain any words or information you do not clearly understand. The nature of the study, risks, inconveniences, discomforts, and other important information about the study are provided below.

The person who is in charge of this research study is Julie Haney. This person is called the Principal Investigator. However, other research staff may be involved and can act on behalf of the person in charge.

Purpose of the study
This study is being performed to understand consumers' smart home security and privacy concerns, actions, information sources, and expectations. To gain this understanding, we are conducting a survey of smart home users from across the United States. Study results will contribute to the development of standards that reflect the security and privacy needs and preferences of smart home consumers. The research is funded and conducted by the National Institute of Standards and Technology (NIST).

Why are you being asked to take part?
We are asking you to take part in this research study because you are an adult who lives in the U.S. and are an active user of a smart home device in at least one of the following categories: virtual voice assistants (e.g., Amazon Alexa); smart thermostats (e.g., Nest, Ecobee); smart security devices (e.g., cameras, video doorbells, garage door openers); smart environment sensors (e.g., smoke or leak detectors); and smart lighting (e.g., lightbulbs, lighting systems).

Study Procedures:
If you take part in this study, you will be asked to do the following:

- In the online survey, select the types/categories of smart home devices that you own or use in your household. You will be asked to complete the survey based on your experiences with devices in only one of those device categories.
- You will be asked questions about your views on the security and privacy of your smart home devices, including: your security and privacy concerns (if any); what actions you take to alleviate those concerns (if any); who you think is responsible for the security and privacy of your devices; and what information sources (if any) you use to learn more about the security and privacy of your devices. You will also be asked some questions about yourself.
- The study should take you approximately 20 minutes to complete.

Total Number of Participants
About **400** individuals will take part in this online survey.

Voluntary Participation / Withdrawal
You do not have to participate in this research study.
You should only take part in this study if you want to volunteer. You should not feel that there is any pressure to take part in the study. You are free to participate in this research or withdraw at any time. There will be no penalty or loss of benefits you are otherwise entitled to receive if you stop taking part in this study. You may withdraw from the study by exiting without submitting the survey. If you exit the survey before submitting, your data will be removed from the research record. However, once you have submitted the survey, your data cannot be removed since there will be no way to associate your response with your identity since survey responses are collected anonymously.

Risks or Discomfort
This research is considered to be minimal risk. That means that the risks associated with this study are the same as what you face every day. There are no known additional risks to those who take part in this study. There is also a very small risk that someone who is not authorized could get access to the data. However, we describe how we will protect your confidentiality in a later section of this information sheet.

Costs
It will not cost you anything to take part in the study.

Privacy and Confidentiality
We will keep your study records private and confidential. Your survey responses will be assigned an identification number that will not be linked back to you. All survey data will be stored on an encrypted computer or hard drive in a locked office.
Certain people may need to see your study records. Anyone who looks at your records must keep them confidential. These individuals include:

- The research team, including the Principal Investigator, study coordinator, and all other research staff.
- Certain government people who need to know more about the study, and individuals who provide oversight to ensure that we are doing the study in the right way.
- Any agency of the federal, state, or local government that regulates this research, including the Office for Human Research Protection (OHRP).

Your identity will be protected to the extent permitted by law, including the Freedom of Information Act. We may publish what we learn from this study. If we do, we will not include your name. We will not publish anything that would let people know who you are. Total confidentiality cannot be guaranteed, since all security measures have vulnerabilities and may be compromised.

Future use of research data and/or specimens
The survey data will be retained for study record keeping per NIST institutional policy. Data will not be used for any additional research studies.

You can get the answers to your questions, concerns, or complaints
If you have any questions, concerns, or complaints about this study or experience an unanticipated problem or research-related injury, call or email Julie Haney at 301-975-6772 or julie.haney@nist.gov.

If you have questions about your rights as a participant in this study or have complaints, concerns or issues you want to discuss with someone outside the research team, call the Research Protections Office (RPO) at (301) 975-5445.

You should only decide to participate if the following is true for you:

I understand the above description of the research and the risks and benefits associated with my participation as a research subject. I understand that by proceeding with this survey I agree to take part in this research and do so voluntarily.

Print this page

« Back Next »

Smart Home Security and Privacy Survey

Throughout the survey, the following terms are used:

- **Smart home device** is a network-connected device (connected via Wi-Fi, Bluetooth, or similar technologies) that is used to remotely and/or more effectively and easily control functions or physical aspects of the home.
- **Smart home device app** is an application on your smartphone, computer, laptop, or tablet that is used to remotely control or access your smart home device.
- In the context of the survey, **security** refers to the technologies and techniques used to protect smart home devices and the data (information) they collect from unauthorized access or digital (cyber) attack. In this survey, "security" is equivalent to "cybersecurity." Physical security related to the home or its occupants is different and will be referred to as "home security."
- **Privacy** refers to the state in which individuals feel free from unwarranted observation or intrusions, including the right of a device owner or user to maintain control over and be assured confidentiality of any personal information that is collected, transmitted, used, and stored while using smart home devices.

« Back Next »

Smart Home Security and Privacy Survey

Smart Home Devices

Which of the following smart home devices do you own or use in your house? (Select all that apply.)
Remember: A smart home device is a network-connected device (connected via Wi-Fi, Bluetooth, or similar technologies) that is used to remotely and/or more effectively and easily control functions or physical aspects of the home.

- [ ] Virtual voice assistants and smart speakers (e.g., Amazon Echo/Alexa, Google Nest Home Hub, Apple HomePod)
- [ ] Thermostats (e.g., Nest, Ecobee)
- [ ] Home security devices (e.g., video doorbells, cameras, door locks, garage door openers)
- [ ] Home environment sensors (e.g., smoke and leak detectors)
- [x] Lighting devices (e.g., lightbulbs, lighting systems). This category does **not** include smart plugs that control lights.

« Back Next »

Smart Home Security and Privacy Survey

Smart Home Devices

Unless otherwise indicated, please answer the following questions based on your lighting devices (e.g., lightbulbs, lighting systems) only.

How many lighting devices (e.g., lightbulbs, lighting systems) do you own or use in your house?

- ( ) 1 device
- ( ) 2 to 3 devices
- ( ) 4 to 5 devices
- ( ) 6 to 7 devices
- ( ) 8 or 9 devices
- ( ) 10 or more devices

Next »

Smart Home Security and Privacy Survey

Unless told otherwise, please answer the following questions for your lighting devices (e.g., lightbulbs, lighting systems) only.
Remember:

- **Security** refers to the technologies and techniques used to protect smart home devices and the data (information) they collect from unauthorized access or digital (cyber) attack. In this survey, "security" is equivalent to "cybersecurity." Physical security related to the home or its occupants is different and will be referred to as "home security."
- The **privacy** of smart home devices refers to the right of a party to maintain control over and be assured confidentiality of personal information that is collected, transmitted, used, and stored during the use of smart home devices.

« Back Next »

Smart Home Security and Privacy Survey

Security and Privacy Concerns and Actions

Regarding what you think is *currently* true about your lighting devices (e.g., lightbulbs, lighting systems), please rate your level of agreement with the following:

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I think that most of these smart home devices are secure.	◯	◯	◯	◯	◯
I think that most of these smart home devices protect my privacy.	◯	◯	◯	◯	◯

« Back Next »

Smart Home Security and Privacy Survey

Security and Privacy Concerns and Actions

How concerned are you with the following for your lighting devices?

	Not at all Concerned	Slightly Concerned	Somewhat Concerned	Moderately Concerned	Extremely Concerned
The security of my smart home devices	◯	◯	◯	◯	◯
The privacy of my smart home devices	◯	◯	◯	◯	◯

« Back Next »

Smart Home Security and Privacy Survey

Security and Privacy Concerns and Actions

Regarding your lighting devices, please rate your level of agreement with the following statements:

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I understand the security risks associated with my smart home devices.	◯	◯	◯	◯	◯
I understand the privacy risks associated with my smart home devices.	◯	◯	◯	◯	◯

« Back Next »

Smart Home Security and Privacy Survey

Security and Privacy Concerns and Actions

For each of the following security-related scenarios involving your lighting devices, please rate your level of concern.

	Not at All Concerned	Slightly Concerned	Somewhat Concerned	Moderately Concerned	Extremely Concerned
A security problem with my smart home data exposing members of my household to identity theft or financial loss.	○	○	○	○	○
A security problem with my smart home device leading to unauthorized access to my other devices (e.g., smartphones, computers, tablets, or other smart home devices).	○	○	○	○	○
A security problem with my smart home device leading to my device being used as part of a botnet.	○	○	○	○	○

« Back Next »

Smart Home Security and Privacy Survey

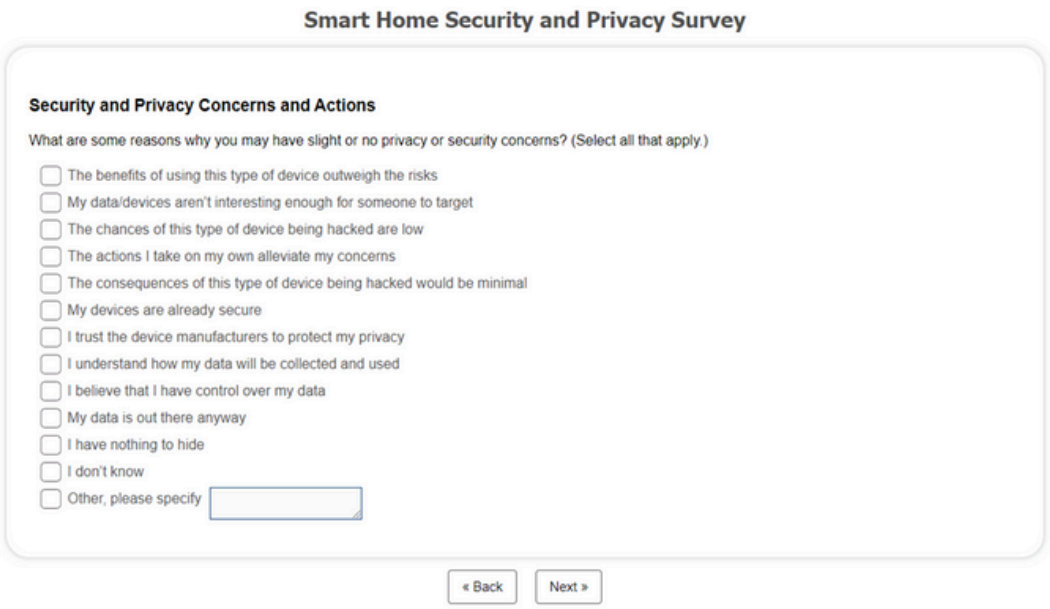
Security and Privacy Concerns and Actions

For each of the following privacy-related scenarios involving your lighting devices, please rate your level of concern.
"Others" can refer to device manufacturers, advertisers, hackers/attackers (unauthorized individuals), the government, or other third-party organizations.

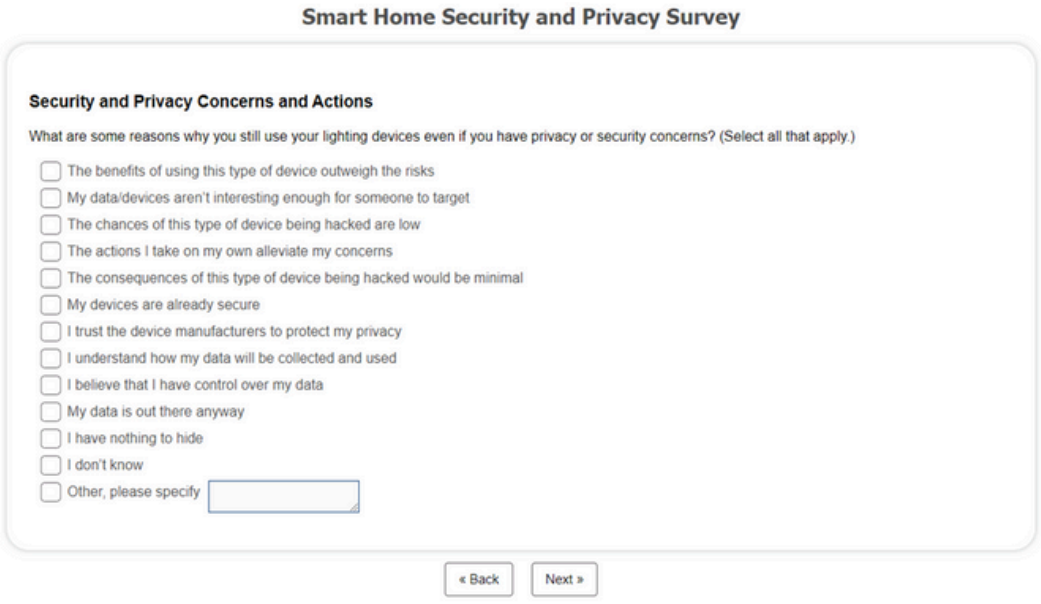
	Not at all Concerned	Slightly Concerned	Somewhat Concerned	Moderately Concerned	Extremely Concerned
Others using my smart home data in ways that I don't expect or authorize.	○	○	○	○	○
Others misrepresenting my smart home data in an inaccurate, insulting, or unflattering manner.	○	○	○	○	○
Having to provide more personal or private information than I feel comfortable with when setting up or using my smart home device.	○	○	○	○	○
Others using my smart home data to uniquely identify members of my household.	○	○	○	○	○
Others using my smart home data to create inferences/assumptions about members of my household that could result in embarrassment or discrimination.	○	○	○	○	○
Others tracking or monitoring my smart home data or usage in a manner that could result in physical harm to members of my household.	○	○	○	○	○
Others tracking or monitoring my smart home data or usage in a manner that could result in a violation of the individual rights of members of my household.	○	○	○	○	○
Others collecting and combining different kinds of smart home data and revealing private things about members of my household.	○	○	○	○	○
Members of my household not having awareness of what data is being collected by my smart home devices.	○	○	○	○	○
Members of my household not having awareness of how data collected by my smart home devices is being used.	○	○	○	○	○

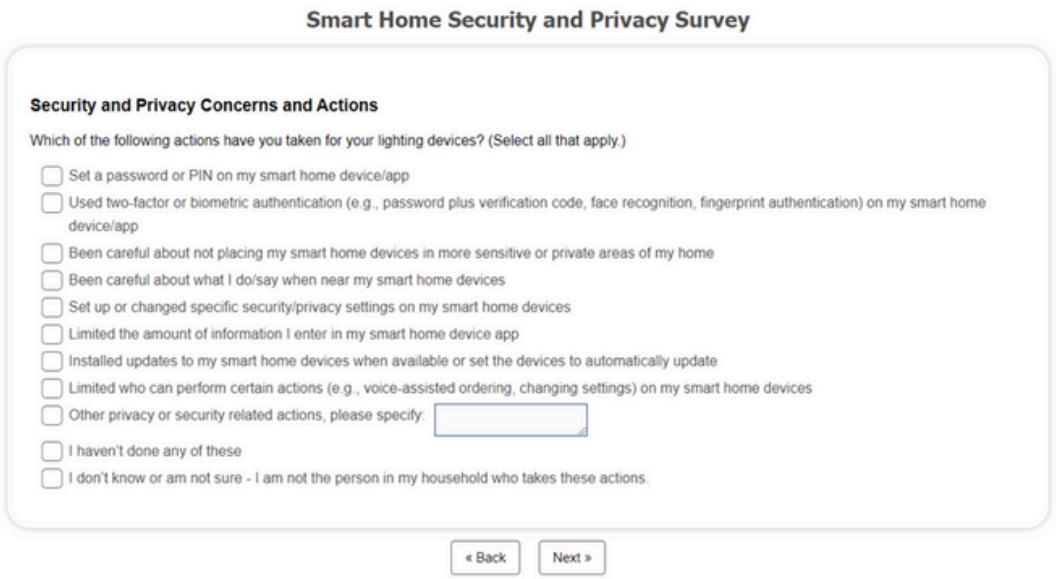
« Back Next »

If respondent selects "Not at all concerned" or "Slightly Concerned" for all of the items in Question 7, they will see this version of the question:



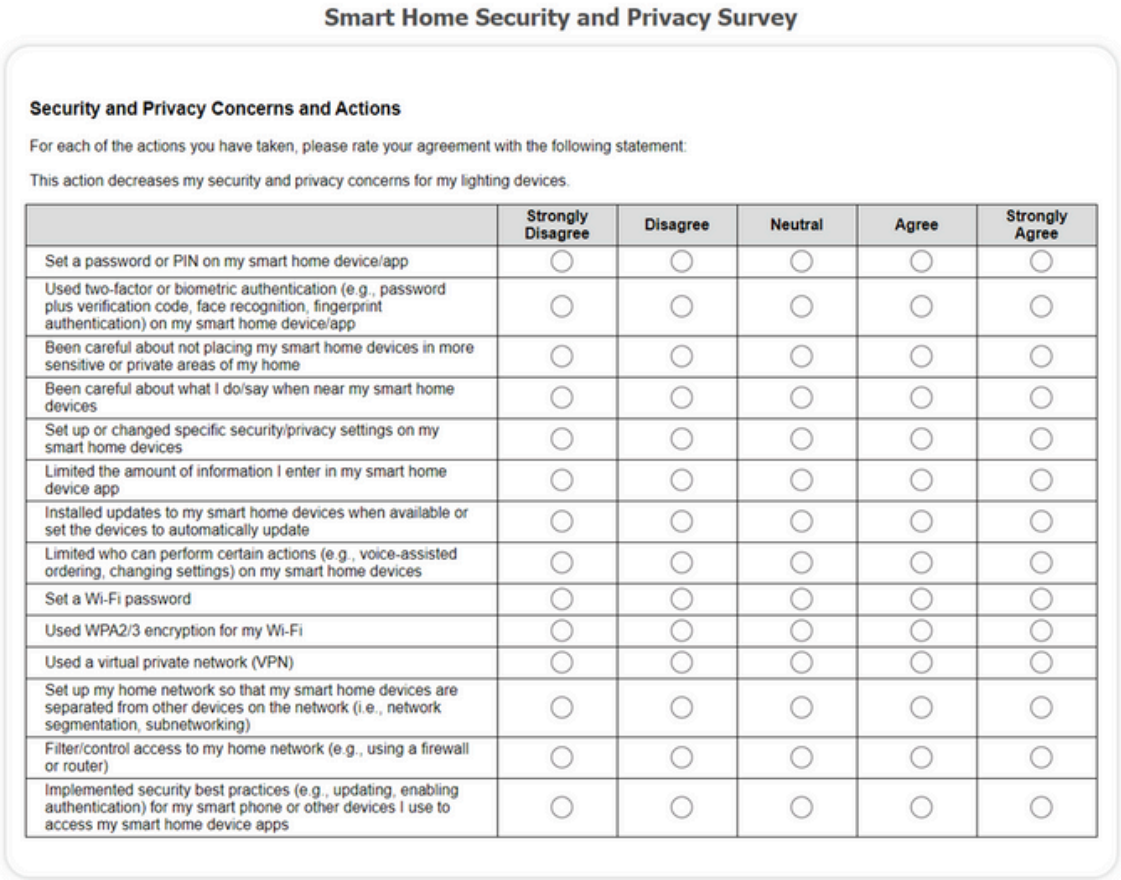
If respondent answers "Somewhat Concerned," "Moderately Concerned," or "Extremely Concerned" for at least one of the items in Question 7, they will see this version of the question:




Smart Home Security and Privacy Survey
Security and Privacy Concerns and Actions
Which of the following actions have you taken for your lighting devices? (Select all that apply.)
Set a password or PIN on my smart home device/app
Used two-factor or biometric authentication (e.g., password plus verification code, face recognition, fingerprint authentication) on my smart home device/app
Been careful about not placing my smart home devices in more sensitive or private areas of my home
Been careful about what I do/say when near my smart home devices
Set up or changed specific security/privacy settings on my smart home devices
Limited the amount of information I enter in my smart home device app
Installed updates to my smart home devices when available or set the devices to automatically update
Limited who can perform certain actions (e.g., voice-assisted ordering, changing settings) on my smart home devices
Other privacy or security related actions, please specify:
I haven't done any of these
I don't know or am not sure - I am not the person in my household who takes these actions.
« Back
Next »


Smart Home Security and Privacy Survey
Security and Privacy Concerns and Actions
Which of the following actions have you taken on your home network (e.g., your home Wi-Fi)? (Select all that apply.)
Set a Wi-Fi password
Used WPA2/3 encryption for my Wi-Fi
Used a virtual private network (VPN)
Set up my home network so that my smart home devices are separated from other devices on the network (i.e., network segmentation, subnetworking)
Filter/control access to my home network (e.g., using a firewall or router)
Implemented security best practices (e.g., updating, enabling authentication) for my smart phone or other devices I use to access my smart home device apps
Other privacy or security related actions, please specify:
I don't do any of these
I don't know or am not sure - I am not the person in my household who takes these actions.
« Back
Next »

Items selected in the two prior questions will be used to populate this question. This question will be skipped if respondents select "I haven't done any of these" or "I don't know or am not sure" for both of those prior questions.



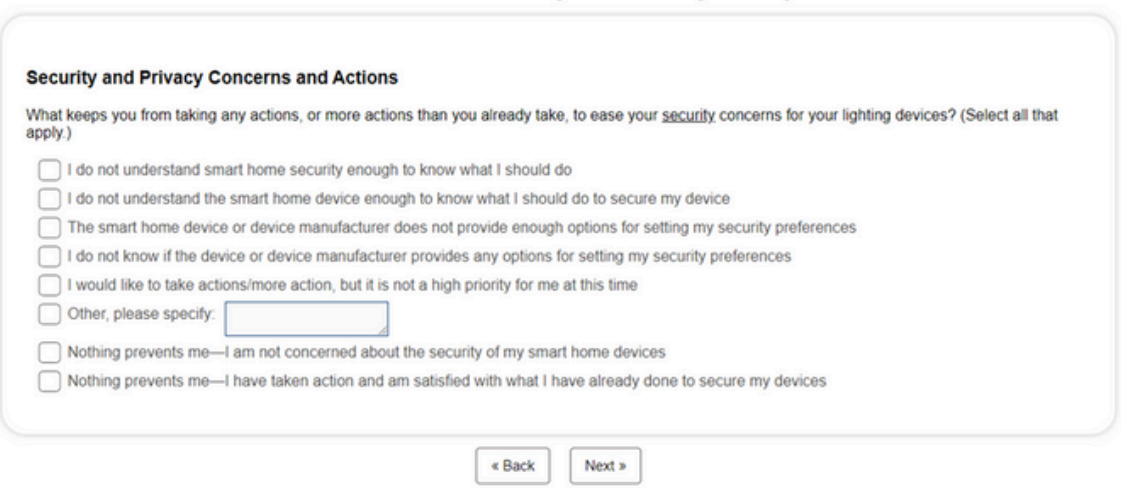
Smart Home Security and Privacy Survey

Security and Privacy Concerns and Actions

For each of the actions you have taken, please rate your agreement with the following statement:

This action decreases my security and privacy concerns for my lighting devices.

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Set a password or PIN on my smart home device/app	○	○	○	○	○
Used two-factor or biometric authentication (e.g., password plus verification code, face recognition, fingerprint authentication) on my smart home device/app	○	○	○	○	○
Been careful about not placing my smart home devices in more sensitive or private areas of my home	○	○	○	○	○
Been careful about what I do/say when near my smart home devices	○	○	○	○	○
Set up or changed specific security/privacy settings on my smart home devices	○	○	○	○	○
Limited the amount of information I enter in my smart home device app	○	○	○	○	○
Installed updates to my smart home devices when available or set the devices to automatically update	○	○	○	○	○
Limited who can perform certain actions (e.g., voice-assisted ordering, changing settings) on my smart home devices	○	○	○	○	○
Set a Wi-Fi password	○	○	○	○	○
Used WPA2/3 encryption for my Wi-Fi	○	○	○	○	○
Used a virtual private network (VPN)	○	○	○	○	○
Set up my home network so that my smart home devices are separated from other devices on the network (i.e., network segmentation, subnetworking)	○	○	○	○	○
Filter/control access to my home network (e.g., using a firewall or router)	○	○	○	○	○
Implemented security best practices (e.g., updating, enabling authentication) for my smart phone or other devices I use to access my smart home device apps	○	○	○	○	○



Smart Home Security and Privacy Survey

Security and Privacy Concerns and Actions

What keeps you from taking any actions, or more actions than you already take, to ease your security concerns for your lighting devices? (Select all that apply.)

- ☐ I do not understand smart home security enough to know what I should do
- ☐ I do not understand the smart home device enough to know what I should do to secure my device
- ☐ The smart home device or device manufacturer does not provide enough options for setting my security preferences
- ☐ I do not know if the device or device manufacturer provides any options for setting my security preferences
- ☐ I would like to take actions/more action, but it is not a high priority for me at this time
- ☐ Other, please specify:
- ☐ Nothing prevents me—I am not concerned about the security of my smart home devices
- ☐ Nothing prevents me—I have taken action and am satisfied with what I have already done to secure my devices

« Back Next »

Smart Home Security and Privacy Survey

Security and Privacy Concerns and Actions

What keeps you from taking any actions, or more actions than you already take, to ease your privacy concerns for your lighting devices? (Select all that apply.)

- ☐ I do not understand smart home privacy (including data collection and use) enough to know what I should do
- ☐ I do not understand the smart home device enough to know what I should do to protect my privacy
- ☐ The smart home device or device manufacturer does not provide enough options for setting my privacy preferences
- ☐ I do not know if the device or device manufacturer provides any options for setting my privacy preferences
- ☐ I would like to take actions/more action, but it is not a high priority for me at this time
- ☐ Other, please specify:
- ☐ Nothing prevents me—I am not concerned about the privacy of my smart home devices
- ☐ Nothing prevents me—I have taken action and am satisfied with what I have already done to protect my privacy

« Back Next »

Smart Home Security and Privacy Survey

Responsibility

Please indicate your agreement with the following statements about your lighting devices:

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I think that the manufacturers currently provide me with enough options to set my own security preferences.	○	○	○	○	○
I think the manufacturers currently provide me with enough options to set my own privacy preferences.	○	○	○	○	○
I have to take action on my own to secure my smart home devices.	○	○	○	○	○
I have to take action on my own to protect my privacy when using my smart home devices.	○	○	○	○	○

« Back Next »

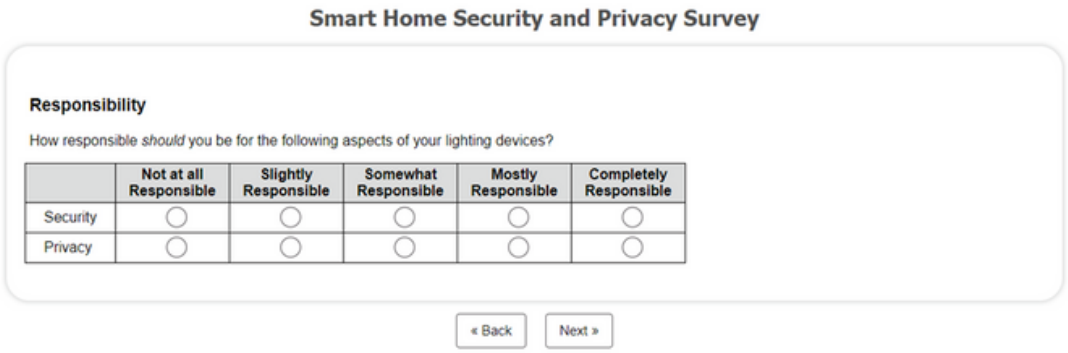
Smart Home Security and Privacy Survey

Responsibility

How responsible are you *currently* for the following aspects of your lighting devices?

	Not at all Responsible	Slightly Responsible	Somewhat Responsible	Mostly Responsible	Completely Responsible
Security	○	○	○	○	○
Privacy	○	○	○	○	○

« Back Next »



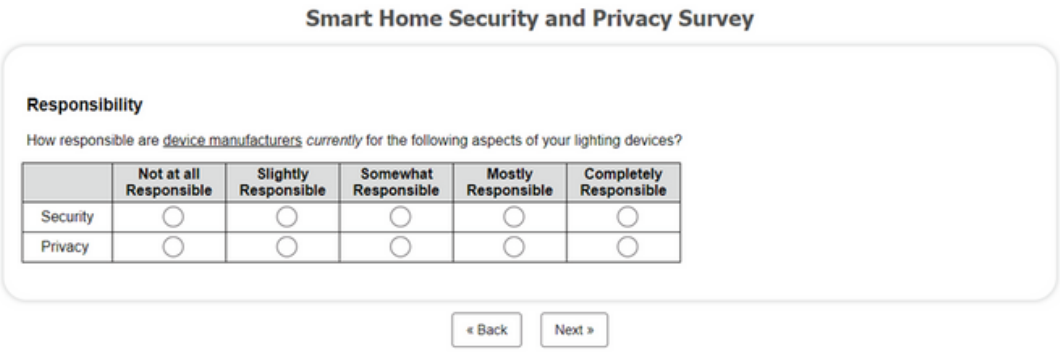
Smart Home Security and Privacy Survey

Responsibility

How responsible *should* you be for the following aspects of your lighting devices?

	Not at all Responsible	Slightly Responsible	Somewhat Responsible	Mostly Responsible	Completely Responsible
Security	○	○	○	○	○
Privacy	○	○	○	○	○

« Back Next »



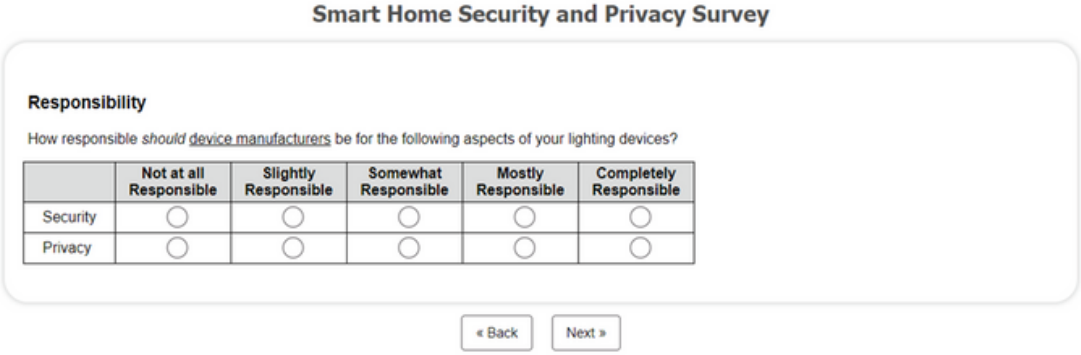
Smart Home Security and Privacy Survey

Responsibility

How responsible are device manufacturers *currently* for the following aspects of your lighting devices?

	Not at all Responsible	Slightly Responsible	Somewhat Responsible	Mostly Responsible	Completely Responsible
Security	○	○	○	○	○
Privacy	○	○	○	○	○

« Back Next »



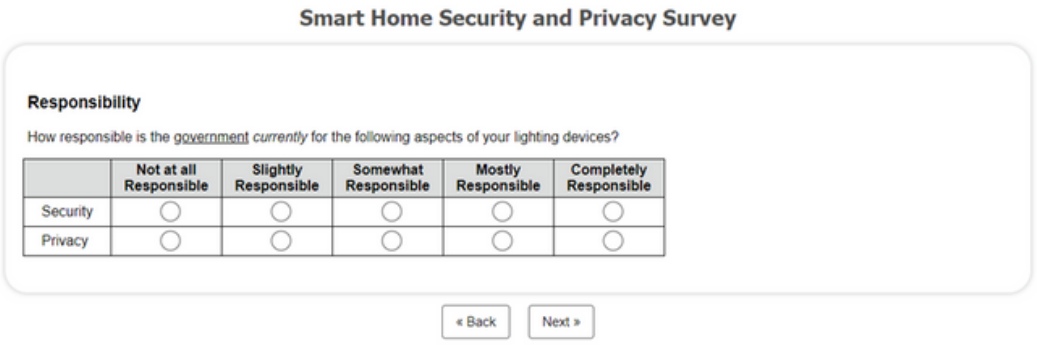
Smart Home Security and Privacy Survey

Responsibility

How responsible *should* device manufacturers be for the following aspects of your lighting devices?

	Not at all Responsible	Slightly Responsible	Somewhat Responsible	Mostly Responsible	Completely Responsible
Security	○	○	○	○	○
Privacy	○	○	○	○	○

« Back Next »



Smart Home Security and Privacy Survey

Responsibility

How responsible is the government *currently* for the following aspects of your lighting devices?

	Not at all Responsible	Slightly Responsible	Somewhat Responsible	Mostly Responsible	Completely Responsible
Security	○	○	○	○	○
Privacy	○	○	○	○	○

« Back Next »

Smart Home Security and Privacy Survey

Responsibility

How responsible *should* the government be for the following aspects of your lighting devices?

	Not at all Responsible	Slightly Responsible	Somewhat Responsible	Mostly Responsible	Completely Responsible
Security	○	○	○	○	○
Privacy	○	○	○	○	○

« Back Next »

Smart Home Security and Privacy Survey

Responsibility

Rate your agreement with the following statements:

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I feel able to protect my smart home device's security.	○	○	○	○	○
I feel able to protect my privacy when using my smart home device.	○	○	○	○	○
I am willing to put in the effort to protect my privacy when using my smart home device.	○	○	○	○	○
I am willing to put in the effort to secure my smart home device.	○	○	○	○	○

« Back Next »

Smart Home Security and Privacy Survey

Security & Privacy Information Sources

How do you *currently* learn about the security and privacy features of your lighting devices? (Select all that apply.)

- ☐ Manufacturer's website
- ☐ Online retailer website product description (e.g., Amazon or Best Buy websites)
- ☐ Online forums discussing smart home devices (e.g., Reddit)
- ☐ Social media
- ☐ Family or friends
- ☐ News articles/stories
- ☐ Product package
- ☐ Device privacy policy or user level agreement
- ☐ Information included on an in-store retail outlet's product shelf label or display
- ☐ Security vulnerability databases/repositories
- ☐ My workplace
- ☐ Internet service provider
- ☐ Videos, webinars, or other online training
- ☐ Other, please specify:
- ☐ I don't currently seek out security and privacy information about my devices

« Back Next »

Smart Home Security and Privacy Survey

Security & Privacy Information Sources

In what ways *would you like to* learn about the security and privacy features of your lighting devices in the future? (Select all that apply.)

- [ ] Manufacturer's website
- [ ] Online retailer website
- [ ] Online forums discussing smart home devices (e.g., Reddit)
- [ ] Social media
- [ ] Family or friends
- [ ] News articles/stories
- [ ] Product package
- [ ] Device privacy policy or user level agreement
- [ ] Information included on an in-store retail outlet's product shelf label or display
- [ ] Security vulnerability databases/repositories
- [ ] My workplace
- [ ] Internet service provider
- [ ] Videos, webinars, or other online training
- [ ] Other, please specify:
- [ ] I'm not interested in learning more about the security and privacy features of my devices

« Back Next »

Smart Home Security and Privacy Survey

Security & Privacy Information Sources

How likely are you to use the following information to inform your future purchases of lighting devices?

	Very Unlikely	Unlikely	Neutral	Likely	Very Likely
Information on the security and privacy risks of my smart home device	○	○	○	○	○
Information on the device manufacturer's data practices, including collection and use of data	○	○	○	○	○
Information on what security features and options are included in my device	○	○	○	○	○
Information on what privacy features and options are included in my device	○	○	○	○	○
Information on whether the product has met some kind of minimum security or privacy standards	○	○	○	○	○

« Back Next »

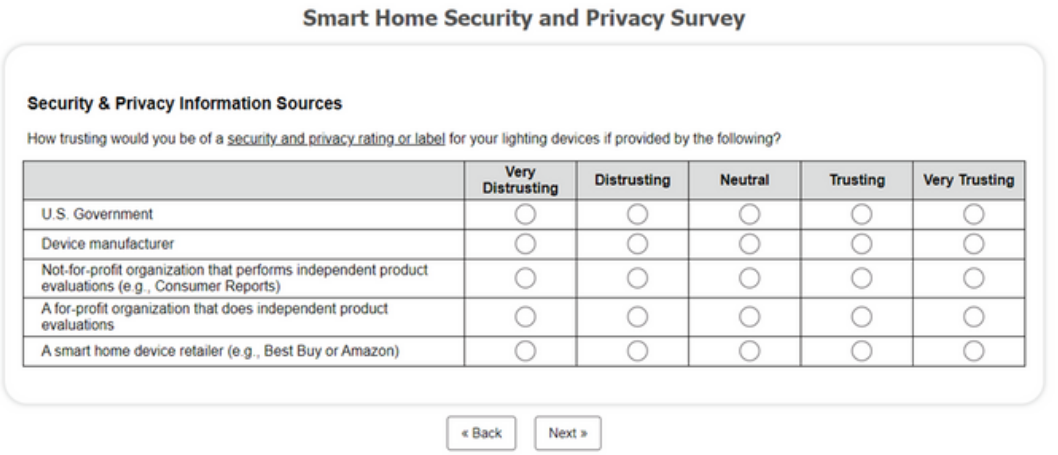
Smart Home Security and Privacy Survey

Security & Privacy Information Sources

How likely would you be to act on the following information for your lighting devices?

	Very Unlikely	Unlikely	Neutral	Likely	Very Likely
Recommendations on how to better secure my smart home device (e.g., by configuring device security options)	○	○	○	○	○
Recommendations on how to better secure my home network	○	○	○	○	○
Recommendations on how to better protect my privacy when using my smart home device (e.g., by configuring device privacy options)	○	○	○	○	○

« Back Next »



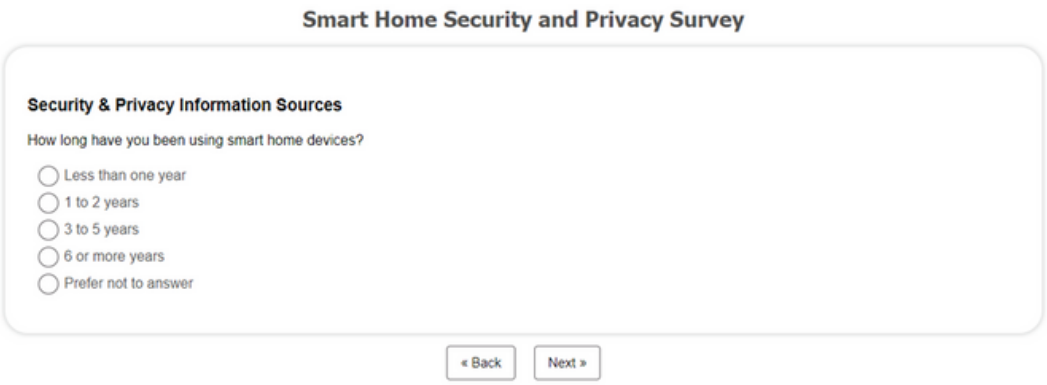
Smart Home Security and Privacy Survey

Security & Privacy Information Sources

How trusting would you be of a security and privacy rating or label for your lighting devices if provided by the following?

	Very Distrusting	Distrusting	Neutral	Trusting	Very Trusting
U.S. Government	○	○	○	○	○
Device manufacturer	○	○	○	○	○
Not-for-profit organization that performs independent product evaluations (e.g., Consumer Reports)	○	○	○	○	○
A for-profit organization that does independent product evaluations	○	○	○	○	○
A smart home device retailer (e.g., Best Buy or Amazon)	○	○	○	○	○

« Back Next »



Smart Home Security and Privacy Survey

Security & Privacy Information Sources

How long have you been using smart home devices?

- ○ Less than one year
- ○ 1 to 2 years
- ○ 3 to 5 years
- ○ 6 or more years
- ○ Prefer not to answer

« Back Next »

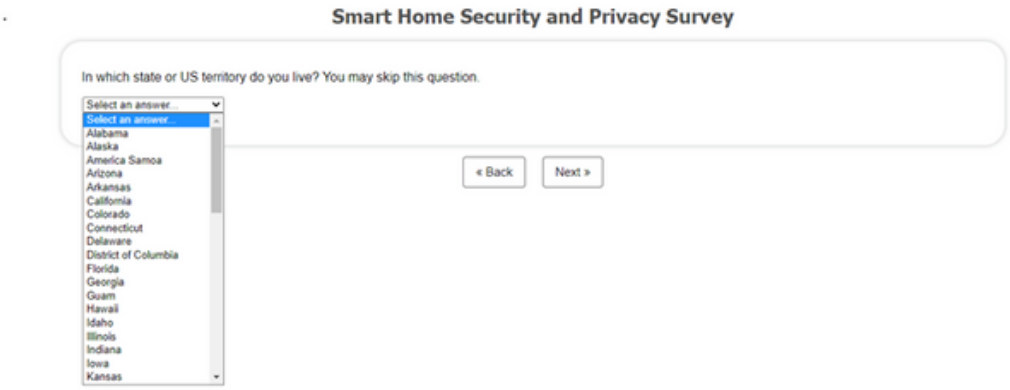
Smart Home Security and Privacy Survey

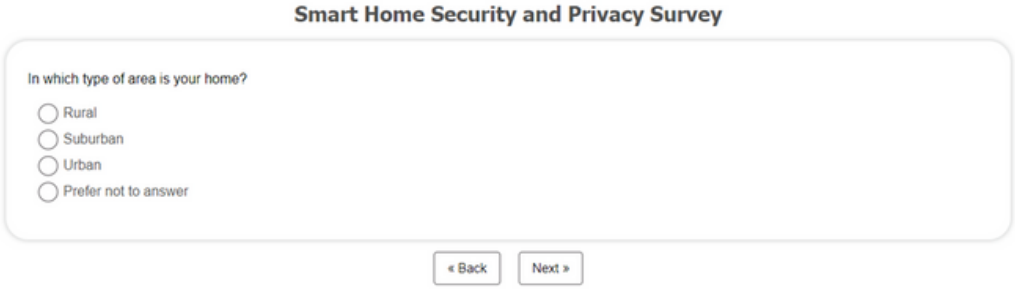
Security & Privacy Information Sources

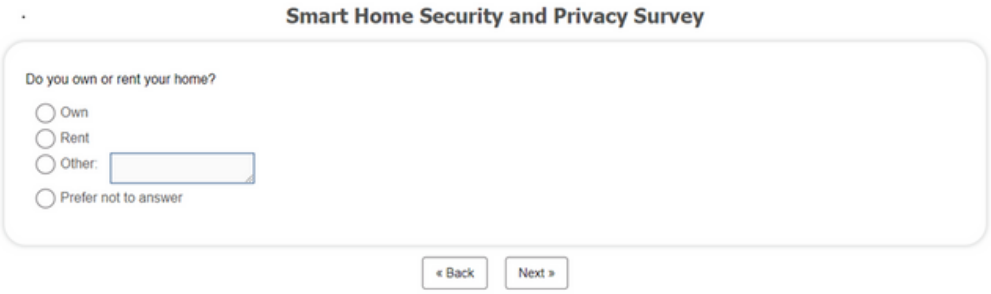
How would you best describe your role with respect to your smart home devices?

- ○ I am an administrator of smart home devices in my household - I installed the devices or I am the one who configures the devices or troubleshoots when something goes wrong.
- ○ I am an active user of the smart home devices but not an administrator
- ○ Other, please specify:

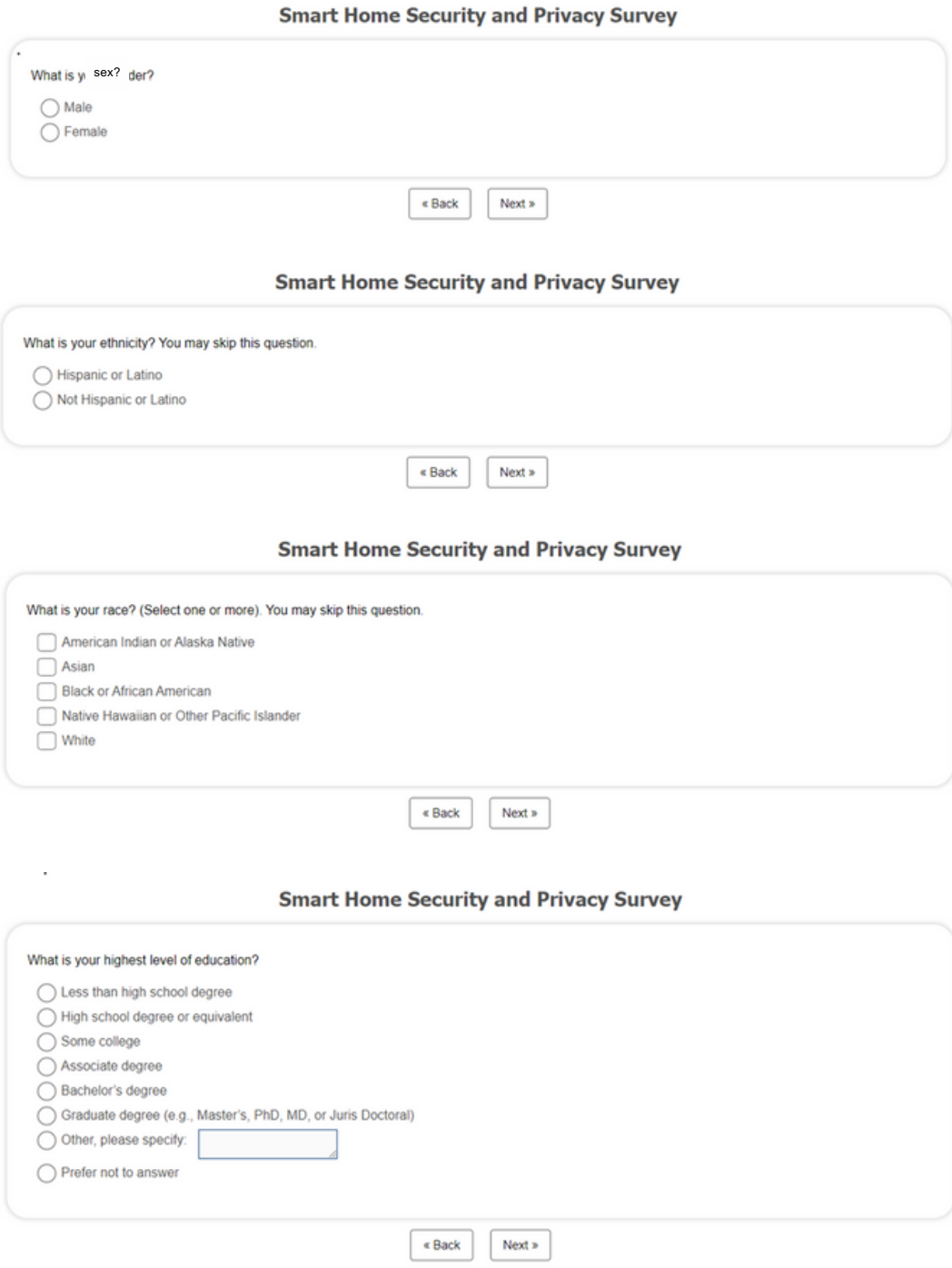
« Back Next »

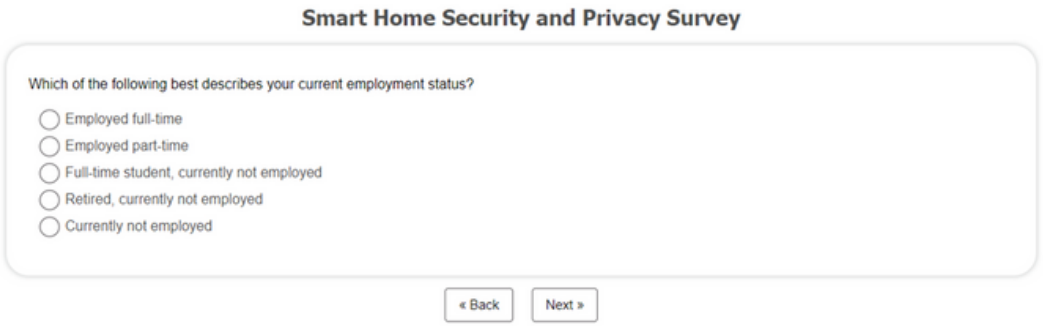

Smart Home Security and Privacy Survey
In which state or US territory do you live? You may skip this question.
Select an answer...
Select an answer...
Alabama
Alaska
America Samoa
Arizona
Arkansas
California
Colorado
Connecticut
Delaware
District of Columbia
Florida
Georgia
Guam
Hawaii
Idaho
Illinois
Indiana
Iowa
Kansas
« Back
Next »

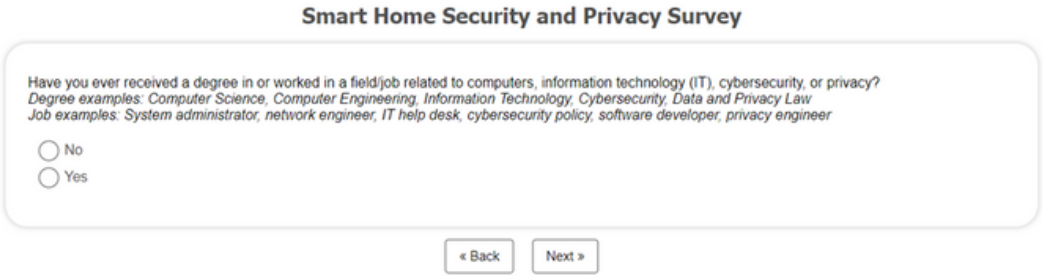

Smart Home Security and Privacy Survey
In which type of area is your home?
Rural
Suburban
Urban
Prefer not to answer
« Back
Next »


Smart Home Security and Privacy Survey
Do you own or rent your home?
Own
Rent
Other:
Prefer not to answer
« Back
Next »

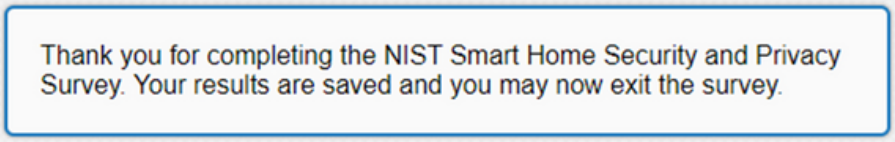

Smart Home Security and Privacy Survey
What is your age range? You may skip this question.
18 to 24
25 to 34
35 to 44
45 to 54
55 to 64
65 or older
Prefer not to answer
« Back
Next »


Smart Home Security and Privacy Survey
What is y sex? der?
Male
Female
« Back
Next »
Smart Home Security and Privacy Survey
What is your ethnicity? You may skip this question.
Hispanic or Latino
Not Hispanic or Latino
« Back
Next »
Smart Home Security and Privacy Survey
What is your race? (Select one or more). You may skip this question.
American Indian or Alaska Native
Asian
Black or African American
Native Hawaiian or Other Pacific Islander
White
« Back
Next »
Smart Home Security and Privacy Survey
What is your highest level of education?
Less than high school degree
High school degree or equivalent
Some college
Associate degree
Bachelor's degree
Graduate degree (e.g., Master's, PhD, MD, or Juris Doctoral)
Other, please specify:
Prefer not to answer
« Back
Next »


Smart Home Security and Privacy Survey
Which of the following best describes your current employment status?
Employed full-time
Employed part-time
Full-time student, currently not employed
Retired, currently not employed
Currently not employed
« Back
Next »


Smart Home Security and Privacy Survey
Have you ever received a degree in or worked in a field/job related to computers, information technology (IT), cybersecurity, or privacy?
Degree examples: Computer Science, Computer Engineering, Information Technology, Cybersecurity, Data and Privacy Law
Job examples: System administrator, network engineer, IT help desk, cybersecurity policy, software developer, privacy engineer
No
Yes
« Back
Next »


Smart Home Security and Privacy Survey
What was your total household income before taxes during the past 12 months? (Do not include income of dependents or unrelated household members). You may skip this question.
Less than $25,000
$25,000 to $34,999
$35,000 to $49,999
$50,000 to $74,999
$75,000 to $99,999
$100,000 to $149,999
$150,000 to $199,999
$200,000 to $299,999
$300,000 to $399,999
$400,000 and above
Prefer not to answer
« Back
Submit


Thank you for completing the NIST Smart Home Security and Privacy Survey. Your results are saved and you may now exit the survey.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

CONTACT US:

https://csrc.nist.gov/projects/human-centered-cybersecurity
human-cybersec@nist.gov