User-Centric Privacy Controls for Smart Homes

CHOLA CHHETRI, George Mason University, USA
VIVIAN MOTTI, George Mason University, USA

The widespread adoption of smart home devices (SHD) has increased privacy concerns among users, yet user-friendly controls are lacking. While there is a large body of research focused on understanding privacy concerns and threat models of SHD users, there is limited research so far aimed at informing the development of privacy controls in SHDs. This paper presents the results of 25 interviews focused on characterizing the users' needs for privacy controls. Through qualitative analysis of interview data, we present 7 design factors and 32 sub-factors for the design of privacy controls in SHDs. The interview findings informed the design of a survey that was deployed to 440 adult SHD users to gain quantitative insights on privacy control requirements and to complement the interview findings. Based on the findings, we discuss a privacy control framework that guides designers towards user-centric privacy controls.

CCS Concepts: • **Security and privacy → Usability in security and privacy**; • **Human-centered computing → Empirical studies in HCI**.

Additional Key Words and Phrases: smart home, smart home devices, privacy, privacy controls, interviews, user studies

ACM Reference Format:
Chola Chhetri and Vivian Motti. 2022. User-Centric Privacy Controls for Smart Homes. In *Proc. ACM Hum.-Comput. Interact. 6, CSCW2, Article (To appear).* ACM, New York, NY, USA, 35 pages. https://doi.org/10.1145/nnnnnnn

1 INTRODUCTION

Smart home devices (SHDs) provide consumers with convenient services and safety features through smart locks, smart bulbs for light controls, baby monitors with surveillance cameras, and entertainment through smart TVs and speakers [21, 46]. In general, Internet of Things (IoT) devices are considered SHDs, as long as they are used in the context of a private household [47, 56]. SHDs have gained popularity in recent years. As consumers invest more in home automation services, SHDs are expected to reach the homes of more than 1.4 billion people by 2024 [68]. SHDs vary in the device format and specific purposes, however their overarching goal is to facilitate everyday life activities with convenient features, services on demand, information and resources [55]. With the growth of high speed 5G networks, the smart-home ecosystem is also expected to continue growing [41]. SHDs bring disruptive changes to traditional industries [13] thanks to: (1) their intimate and inconspicuous presence on users' lives, (2) large potential to collect data –continuously and from multiple streams– and (3) capability to adapt the environment and services with features and information that meet users' needs on demand.

Locks, cameras, and speakers are examples of Internet-connected devices in a smart home. They serve as intelligent personal assistants that make the home "smarter" by bringing convenient

CSCW'22, October, 2022, Virtual

ACM ISBN 978-1-4503-XXXX-X/18/06…$15.00
https://doi.org/10.1145/nnnnnnn

services to residents [50]. SHDs are not only continuously collecting data from users and their surroundings, but also exchanging information directly through the web, often with third-party commercial services on the cloud, such as Google, Amazon, or Apple [7, 40]. The requests for web services and data exchange pose risks to users' privacy and security [49, 70]. Such risks affect not only smart home residents, but also their guests and bystanders [48].

By having access to multiple data streams in a continuous way, many SHDs access information that is private, confidential and personally identifiable. When aggregated, the analysis and processing of data streams altogether lead to inferences about users' behaviors and predictions. Data access, forecast, and inferences summed with the transmission of private information from users to external services exacerbate privacy risks for end users [31, 64] and security threats of SHDs [74]. Although US users are willing to exchange personal information to obtain tangible benefits, they are also cautious about disclosing personal information and feel dissatisfied with the current approach adopted by industry in what regards the usage of data collected [58].

Many researchers have conducted studies to decipher users threat models of SHDs and privacy concerns regarding SHDs. However, even though smart home devices are widespread, the design of effective privacy controls remains an open challenge. To devise user-centric privacy controls for smart homes, joint efforts that combine technical [43, 60] and legal aspects [17] as well as socio-technical and user-centric approaches [9, 14, 72] are needed. Among the former, the literature reports work on network defenses, cryptographic models, and machine learning models to classify suspicious activities [1, 4, 30]. In the latter, the methods used to characterize users' concerns include interviews, surveys, participatory design, and focus groups [34, 45, 69].

Despite substantial advances focused on understanding users' concerns [22, 73, 74], the translation of users' privacy concerns into user interface and design decisions for customizable privacy controls is still in exploratory phases. So, an in-depth investigation into privacy controls expected by users is necessary to suggest practical design recommendations to aid the development of privacy-enhanced SHDs.

Thus, to investigate SHD privacy controls desired by users, we interviewed 25 participants and analyzed the interviews' transcripts. We performed thematic analysis of privacy controls expectations of users, resulting in seven design factors and 32 sub-factors from the coding of user interface controls desired by users. We used the interview findings to inform the design of a survey deployed to 440 US adults to confirm the findings of the interviews.

The contributions of this paper are: (1) unpacking the privacy controls desired by users of SHDs, and (2) devising a privacy control framework to help developers to implement user-centric privacy controls.

2 RELATED WORK

The adoption of smart home devices grows thanks to their reduction in price and increasing popularity. As electronics become smaller, home appliances also integrate more sensors, amplifying their potential for data collection and embedded 'intelligence'. Smart devices include thermostats, energy monitoring switches, personal assistants, doorbells, smart locks and smart lights. By collecting users' data, such devices become more integrated in users' lives, providing them with convenient services. Despite their advantages, SHDs also lead to several privacy concerns due to their information processing capabilities, heavy reliance on continuous data collection, and exchange of information with external services. The novelty of SHDs also challenges the implementation of privacy-enhanced technologies, since privacy risks are not always known and regulatory practices are either limited or lacking. For example, the General Data Protection Regulation (GDPR) of European Union (EU) is seen as a strict data protection regulation, but it allows exclusion of domestic data practices through its household exemption clause [33]. In the US, there are many data protection regulations, such as Health Insurance Portability and Accountability Act (HIPAA), but they fall short in protecting even the health information collected from SHDs due to inadequate definition of 'protected health information' [24].

The scientific literature reports several contributions dedicated to investigate privacy concerns from a user-centric perspective. Prior work has focused on both characterizing users' concerns and addressing it with technical contributions and privacy controls. Concerning the methodological approaches employed in usable privacy, prior studies collected data using multiple methods, such as: interviews [9, 72], surveys [14, 43], focus groups [18], analysis of online reviews[21], co-design [73, 74] and evaluation [22], case studies [17, 60] and systematic reviews [20, 41].

2.1 Privacy

Privacy has been extensively investigated in past years. Clarke (1999) defines four dimensions of privacy: privacy of a person, privacy of personal behavior, privacy of personal communication and privacy of personal data [23]. Due to privacy being a multidimensional [2, 3, 62] and contextual concept [52], the research community has tackled it from different angles, covering mathematical aspects for differential privacy [25], conceptual, economical costs of privacy risks [26, 29], legal [56], technical [43], behavioral [34] and cultural aspects [14, 40].

Information privacy is defined as combination of privacy of personal communication and privacy of personal data [8]. The information privacy concerns multilevel framework argues that information privacy concerns (IPC) involve four constructs (individual IPC, group IPC, organizational IPC, and societal IPC), each impacted by multiple factors, such as individual differences, group dynamics, organizational environment, and government involvement [8].

Solove's taxonomy of privacy harms is widely used to understand and characterize various privacy problems. It identifies the major activities leading to privacy violations and categorizes them into four groups: (1) Information collection (surveillance and interrogation), (2) Information processing (aggregation, identification, insecurity, secondary use and exclusion), (3) Information dissemination (breach of confidentiality, disclosure, increased accessibility, blackmail, appropriation, and distortion), and (4) Privacy invasion (intrusion and decisional interference) [61].

2.2 Users' Concerns

Using online questionnaires, Cannizzaro et al. (2020) surveyed more than 2000 UK residents to understand trust aspects in the context of smart home. They acknowledged the risks to privacy and security of the smart home residents but found lack of clarity in the consumers' perspectives about the meaning and value proposition of a smart home [14].

Bleaney et al. (2018) applied machine learning algorithms to analyze Amazon reviews and identified safety concerns around baby products [10]. Similarly, Winkler et al. (2016) extracted Amazon reviews using smoke word list and identified safety concerns about toys [67]. Linden et al. (2020) conducted a review analysis of pet wearables [65] and found that users mentioned privacy concerns. Similarly, researchers analyzed reviews of smart home devices [21] and found that users of smart home hubs were concerned about data collection and leakage of private conversations.

Researchers have interviewed users and found that privacy concerns of users are associated with loss of control, attacks to data and services, trade-offs between functionality and security, and societal implications [9, 45, 48, 72–74]. With 42 interviews, Zimmermann et al. (2019) provided recommendations for privacy in SHDs [74]. Zheng et al. (2018) interviewed 11 participants and found that perceived convenience and connectedness lead consumers to purchase and use SHDs. Their results also indicated that privacy-related behaviors include the choice of manufacturer and Internet provider [73]. The concerns identified were related to advertisers and government. The usage of the data by external entities depend on perceived benefits. The trust on vendors is not verified and the risks of inferences are unknown for non-audio/visual devices. Recommendations have also been provided [73]. Mao (2019) interviewed five participants; they found that the risk of privacy breach is tied to secret data collection and that *lack of control* is a barrier for adoption [45].

Birchley et al. (2017) interviewed 20 participants. They found that the concerns around physical privacy reduce acceptance of SHDs [9]. They recommended that users should not be burdened with a lot of controls, since privacy risks cannot necessarily be resolved by them even when an option to choose is provided [9]. Zeng et al. (2017) interviewed 15 participants and noted gaps in users' threat models due to a poor understanding of technical aspects of smart homes. Their analysis of the interviewees' responses indicates that users were aware of some security issues and applied ad hoc mitigation strategies [72]. Additionally, imbalance of power between the home administrator and residents with regards to privacy controls was also noted [72]. Because privacy in the context of a smart home affects bystanders as well, Marky et al. (2020) interviewed guests or visitors. The 21 young adults interviewed shared concerns similar to those of residents; however, they lacked an understanding about data usage or potential controls [48].

Although there is a lack of an instrument to measure information privacy concerns specific to smart home users, prior work utilizes Internet Users' Information Privacy Concerns (IUIPC) [44] to gauge the level of privacy concerns among participants. The IUIPC is a 10-item Likert scale that measures privacy concern using three constructs: Awareness, Control and Collection. In our work, we used this validated scale to measure participants' level of privacy concern.

2.3 Privacy Controls

From a technical perspective, Lin and Bergmann (2016) surveyed privacy solutions and listed key requirements for SHDs. According to them, a gateway architecture is appropriate to manage resource-constrained devices. They also recommend automatic updates of firmware to maintain a secure operating system [43].

Past research has identified lack of privacy controls as a barrier for SHD adoption [38, 42]. Some solutions have been developed in this regard. For example, Emami-Naeini et al. (2019) proposed prototype privacy labels to help users integrate privacy into their IoT device purchase decisions [27]. Privacy labels facilitate regulations, however they serve as a proxy to indicate how privacy-compliant a device is, and do not fully address the issues.

As smart home technologies become more pervasive, the threats, risks and implications to users' privacy increase [57]. Still, due to the novelty of the technology, users' concerns are not fully understood [21]. In addition, privacy risks in smart homes are unclear and mitigation and prevention strategies are unknown [18]. Stakeholders have little to no guidance when implementing new technologies. Strategies to incorporate privacy by design are lacking, as well as evaluation approaches. Prior research shows that user behavior is poorly understood [20], yet it is important to consider users' mental models and attitudes to devise privacy-enhancing controls that are more likely to be accepted, adopted and used in an effective and sustained way.

Research into privacy controls desired by users has recently gained momentum. Yao et al. (2019) performed a co-design study to identify six factors for privacy designs of smart home privacy controls: data transparency and control, security, safety, usability, system intelligence, and modality [70]. This study is a starting point to contribute to user-centric solutions for privacy controls in SHDs. In another study that examined privacy perceptions of smart home bystanders, Yao et al. (2019) made three design suggestions for privacy: transparency, expressing preferences, and different modes [71]. Haney et al. (2020) interviewed administrators and users to investigate user concerns, mitigations and wish lists. They found that users desired data collection transparency, privacy and security controls, security feature transparency, and assistance [35]. In a study aimed at understanding smart home adoption and clustering consumers purchase considerations, Barbosa et al. (2020) also examined desired privacy features of consumers and coded them as: control, transparency, access control, consent, strong security, no data collection, no third parties, deletion, identity protection, offline mode, and guarantees of privacy and security [6].

Study on SHD privacy controls is still in exploratory phase. Design factors, wish lists and feature categories have been explored, but gap exists in how to translate those design factors into user interface design. This paper aims to bridge this gap by generating factors and sub-factors containing privacy controls that can be translated into user interface design[19].

2.4 Commercial Tools

There are limited number of commercial tools available for users to manage privacy in the context of a smart home. Trutzbox [15] is a tool that offers end-to-end encryption, content filter, firewall, antivirus, intrusion prevention, and tracking protection for Internet users [15]. Although not designed specifically for the smart home environment, this tool provides features that a smart home network could benefit from. However, at the time of writing this paper, this tool is available only in the German market. Similarly, another tool Fing [1] provides app and hardware box that monitors home network to detect presence, find out open ports and block unrecognized devices; however, it lacks other privacy-specific solutions at the time of writing this paper.

Aretha [59] was developed as a privacy assistant that included network aggregator, tutor and firewall features; however, this tool was for research purposes only. Similarly, another software designed for research purposes is IoT Inspector [2], which can find IoT devices in the network, display domain namess that IoT devices are communicating with, and visualize network traffic [37].

2.5 Distinction from Prior Work

It is evident from literature that users and researchers have expressed the need for privacy controls. While prior research has explored that users seek transparency, security, privacy and the like, user-centric privacy controls for user interface design of smart home devices are sparse. To bridge this gap, our paper focuses on deciphering the user interface controls desired by participants to mitigate their privacy concerns. Through in-depth interviews, we decipher the privacy controls expected by SHD users. This paper presents 7 design factors and 32 sub-factors analyzed from over two hundred requirements for privacy of SHDs. We also complement and validate the findings of the interviews through a survey. Adopting a user-centric approach, we develop a privacy control framework that guides designers towards creating privacy controls that meet users' privacy expectations in SHDs.

3 METHOD

We used sequential mixed-methods approach [28], in which the findings from interviews informed the design of a survey. We describe both studies in this section.

3.1 Interview Study

To investigate privacy concerns about SHDs and privacy controls expectations of users, we conducted 25 semi-structured interviews. Semi-structured interviews provide a degree of standardization and consistency, while allowing investigation of participant responses in depth and seeking clarifications when necessary [54]. Pilot interviews were conducted before finalizing the interview protocol to test for clarity and make adjustments. The pilot interviews were not included in the analyses.

[1] https://www.fing.com/

[2] https://iotinspector.org/

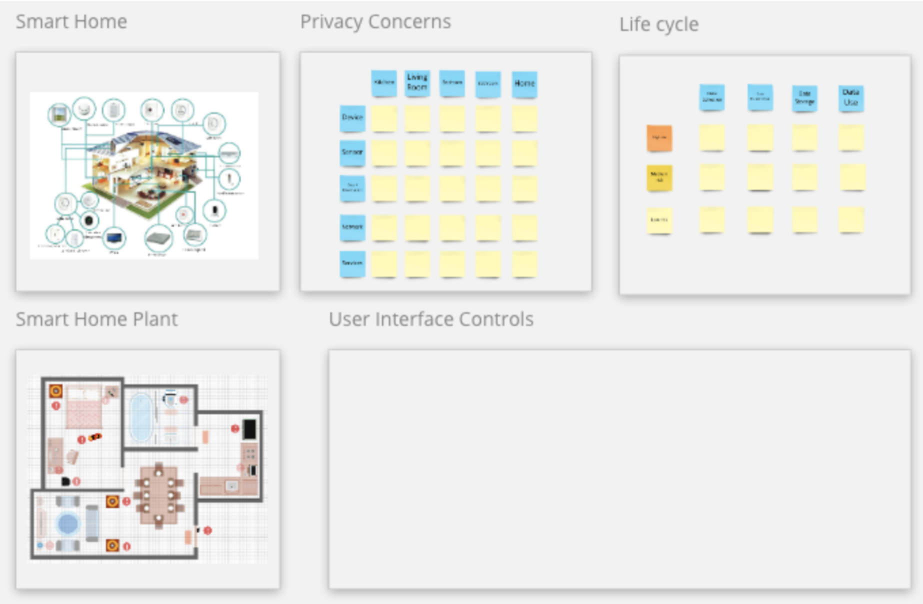


Fig. 1. Screenshot of the frames used in the study. The images on the left illustrate smart homes per floor (top) and per plant (bottom). The pictures were used to ensure all participants had a common understanding about the concept of a smart home and thought broadly about various devices. Sources of the images:[3] [4] On the right, the post its were organized first by rooms, then per life cycle from data collection, to sharing, storage, and use. On the bottom right, participants had a blank frame to propose privacy controls.

3.1.1 Recruitment. Participants were recruited from Northeast region of US. The study was announced online in Twitter and the host institution's event listserv. The announcement included the informed consent and an option to sign up for the study with consent to be contacted for interview. The participants who consented to participate, first completed the demographic form, then answered five questions about their experience and privacy concerns about SHDs. Lastly, they explained their specific concerns about privacy per room (kitchen, living room, bedroom, bathroom, and overall) prompted to think about the device(s), sensor(s), information collected, shared as well as services that could use the data collected. The interview was concluded discussing design recommendations for users of SHDs to gain control over their privacy. Each participant received a USD 20 gift card as compensation.

3.1.2 Participants. Among the 25 participants, 52% (n=13) identified as female, 44% (n=11) as male, and 4% (n=1) as other. Participants' age ranged from 21 to 45 years (M=26.68; SD=5.77). Regarding ethnicity, 36% (n=9) participants reported to be Asian-descendent, 28% (n=7) declared themselves as White (Caucasian), 12% (n=3) were Black (African-American), 12% (n=3) were Hispanic, 8% (n=2) selected two ethnicities (White and Hispanic), and 12% (n=3) selected other.

Concerning the highest educational degree attained, 48% (n=12) participants had a Bachelor's degree, 36% (n=9) had a Master's degree, 8% (n=2) had High School degrees, and 8% (n=2) selected Other. We summarize the participant demographics and the devices owned by participants in Table 1.

As shown in Table 1, participants owned a variety of devices: smart assistants (Amazon Alexa, Google Home), smart lamps (Phillips Hue), smartwatches (Fitbit), etc. Smart speakers were owned

Table 1. Summary of participant demographic and devices owned by participants. In Gender column, M=Male, F=Female, O=Other. In Education column, H=High School or below, B=Bachelor's, M=Master's, O=Other.

Participants	Gender	Age	Education	Devices
P1	M	18-25	B	Fire Stick, Echo
P2	M	26-35	B	Fire TV cube, LIFX light bulb
P3	F	18-25	M	Alexa, Smart Plug
P4	F	26-35	B	Nest Hub, Nest Hub Max, Nest Thermostat
P5	F	18-25	B	Google Home Mini
P6	M	18-25	M	Alexa
P7	F	18-25	O	Google Home Mini
P8	F	18-25	B	Google Homes, Lights
P9	M	26-35	M	Amazon Echoes, Google Nest, Smart Plugs, Google AIY voice kit, Philips HUE lightbulb, LG smart TV
P10	F	26-35	B	Alexa
P11	O	26-35	B	security camera, Google Nest mini, Amazon Echo
P12	F	18-25	B	Google Home Mini
P13	M	26-35	B	Google Nest mini, Amazon Echo, Smoke Detector, Brava Oven, Light bulb
P14	M	18-25	M	Amazon Echo, Smart Plugs, Light Switches, Google Home, Apple homepod mini, ESP 8266 Microcontroller, Web camera, HomeKit
P15	F	36-45	M	Google Nest, Door Bell, Google Nest fire alarms, Google wireless Mesh Router, Google wireless Mesh Router, Google Homes
P16	F	18-25	B	Amazon Echo, Google Home
P17	M	18-25	H	TV, Echo
P18	F	18-25	B	TV, Home
P19	M	26-35	M	Google Home mini
P20	M	18-25	M	Home Security
P21	F	26-35	M	Google Nest Mini (referenced as google dot), Philips HUE lightbulb
P22	F	36-45	M	Low tech thermostat
P23	M	18-25	H	Amazon Echo , Ring Doorbell
P24	M	26-35	B	Amazon Echo, Google Home , Smart Lights, Home security camera, Nest Thermostat, Smart TV, Smart Plugs,
P25	F	26-35	M	Smart plug, Smart lights, Alexa, Siri

by most participants: 72% (n=18). Number of devices per participant ranged from 0-8, with an average of 2.6. Such devices were used frequently (daily, weekly or even a few times a day).

3.1.3 Procedure. The interviews were conducted during October and November of 2020. The online announcement included a link to an online form with an informed consent form to participate in the study and a consent to allow us to contact them for scheduling an interview. Prior to the interview, participants also provided consent for recording. The interview was conducted through Webex[5] and lasted about 60 minutes. Miro[6] (a collaborative tool that serves as a whiteboard) was used to illustrate two examples of smart homes, to frame the study protocol structuring the topics used, and to annotate the participants' comments using digital sticky notes. Figure 1 illustrates the template with the frames used in the study.

The first part of the interview included the following questions:

(1) What is a smart home?
(2) What devices do you use?
(3) What are the benefits of these devices for you?
(4) What are the privacy concerns you have, if any?
(5) What are the privacy controls you use, or would like to use?

In the second part of the interview, to dive in depth into privacy concerns we began the Miro session presenting two illustrations of a smart home (Figure 1 - left). The top image shows a 3-D figure of a two-floor house with several examples of devices, the bottom image illustrates a 2-D house plant with sensors spread in the rooms. The images served to ensure that all participants have a consistent understanding about smart homes, considering a broad definition. Once the SHD concept was explained, participants were invited to think about each room of the house individually (i.e., the kitchen, living room, bedroom, bathroom, or the house in general) as indicated in the central frame (entitled Privacy Concerns) in which they explained their specific privacy concerns related to devices, sensors, data collected, network (data sharing), and services (data usage).

After sharing their specific concerns, participants worked on the right frame (entitled Life Cycle) where they described privacy risks. Specifically, participants described what they considered to be high, medium, or low risk in the process starting with data collection in a smart home, going through transmission and storage, and concluding with data usage. In the last part of the interview, participants suggested recommendations to design controls thinking about best practices and features that should be available in smart home devices.

The interviews were video and audio recorded. The transcripts have been used for data analysis. Also, the post-it notes were extracted for analysis in a comma separated value (CSV) file and screenshots were used for storing the notes. To ensure accessibility, participants who joined by phone could see the shared screen of the moderator with the Miro board but they did not have to type in the sticky notes if they were not comfortable doing so and preferred to speak. Participants who were more comfortable typing refrained from speaking out loud their concerns unless they wanted to provide clarifications or detailed information. Overall, 22 participants preferred to express themselves verbally instead of typing. For three participants who chose to type, the moderator asked to clarify comments when necessary and took notes to minimize the gap between written and verbal comments.

3.1.4 Ethics. Prior to data collection, the study protocol was approved by the institutional review board (IRB) of the host institution. Informed consent for participation in the study was obtained from all participants. Consent was also received from participants prior to audio recording. Confidentiality and anonymity of all participants were ensured by removing any identifying information from transcripts. Participants were referred to by identification codes that included participant (P) numbers, which are used in the Results section to cite quotations.

[5] https://www.webex.com/
[6] https://miro.com/

3.1.5 *Data Analysis.*

The audio recordings were transcribed thoroughly by one researcher and then verified by a second researcher for accuracy. Our approach to thematic analysis was based on the widely used Braun and Clarke (2007) [12] method and included the following steps recursively:

(1) Immerse with the data and identify items of interest.
(2) Generate codes.
(3) Develop themes: Organize codes into potential themes. Examine relationship between themes.
(4) Review potential themes.
(5) Define and name the themes.
(6) Produce the report.

The qualitative data analysis was initiated by two researchers by first going over a few transcripts multiple times to get familiar with the audio and transcripts and then coding five interviews together to generate an initial codebook. The rest of the interviews were then coded iteratively by the two researchers in small batches of three interviews. In each iteration, two researchers coded three interviews independently and then met to resolve differences in code application and agree on new codes to consolidate the codebook. The iterations continued until all 25 interviews were coded. Between the two coders, we achieved an inter-rater reliability of 0.89 using Cohen's kappa, and all disagreements were resolved by consensus. The researchers then examined relationships and patterns among the codes and grouped them into categories and sub-categories, using affinity diagramming. Affinity diagramming [36] was employed to group the codes, and to find similarities and differences across codes.

To analyze privacy controls desired by participants, we followed inductive thematic analysis [12], where the researchers generated the themes from the data using the methods described above. The privacy concerns codes, sub-categories (or sub-factors), and categories (factors) along with their frequencies are detailed in Appendix A.

3.2 Survey Study

The goal of the survey was to gain quantitative insights on privacy controls expectations of participants. The survey was deployed using Amazon Mechanical Turk (MTurk) crowdwork platform as a human intelligence task (HIT) and was restricted to participants from the United States who had task approval rating of 95% or above and had completed at least 100 tasks.

3.2.1 *Design.*

The survey consisted of questions on what privacy controls were expected by participants in smart home devices. Based on the 32 sub-factors of privacy controls from the interview results, the researchers constructed statements about the privacy controls that were presented to survey participants in the form of Likert scale questions. We went through multiple iterations of questionnaire development. Although the initial designs included a variety of questions, such as Yes/No and selection, the authors reached a consensus on Likert scale questions based on the research goal of complementing the findings of the interviews by gaining quantitative insights and also test quantitatively the scale reliability of our interview categories. All the authors of the paper reviewed the questionnaire to ensure that the essence of the related sub-factor was captured in each question.

In the survey, we also asked participants to complete the Internet Users' Information Privacy Concerns (IUIPC) questionnaire [44] and provide demographic information. We included an open ended question at the end of the survey to gather participant feedback on issues experienced in the survey and analyzed each response.

Pilot. We conducted a pilot test of the survey with six volunteer participants and used their feedback to clarify some wordings, minimize technical jargon, and improve the survey flow. This resulted in a refined version of the questionnaire. Data from the pilot study were not used in the final analysis.

Phase 1. We conducted the study in two phases. In phase 1, we collected 50 responses and reviewed all responses. We read and inspected each response manually to determine the quality of responses and to find out if improvements need to be made. We aimed at using participant feedback from this phase to improve the survey and fix any issues to enhance the survey. Phase 1 resulted in no changes to the survey design.

Phase 2. The survey was then deployed to a larger sample of participants to collect 495 responses. Participants were compensated with USD 1.50 for completing the survey.

3.2.2 Survey Workflow. Participants were first presented with information about the study and its informed consent form, with options to agree to participate in the study or deny and quit. To ensure that participants are on the same page, we presented a Wikipedia-adapted definition of smart home[7] that we simplified by reducing technical jargon per consensus among the authors. The definition also included three pictures of smart home devices.

Participants were then asked to identify three pictures of smart home devices correctly out of five pictures presented to them. Participants who did not choose the devices correctly were excluded from the study. This qualification method was inspired from prior literature [6]. Participants were then asked about whether they owned and used smart home devices. They were asked how many and what type of devices they owned. Participants who did not use at least one SHD were excluded from the study. This exclusion criterion was inspired by prior literature [35] to ensure high-quality responses.

Expectations of Privacy Controls. We then asked questions about what privacy controls participants wanted in smart home devices. The privacy controls questions were designed as 5-point Likert scale questions where participants rated their level of agreement with each specific privacy control presented. The privacy control questions represented the privacy control sub-factors from the interview findings discussed in Section 4. We have included all the survey questions in Appendix B

IUIPC and Demographics. To gauge the level of internet privacy concerns among our participants, we asked participants to answer IUIPC questionnaire [44], that consists of ten 7-point Likert questions on three dimensions of information privacy concern: Awareness, Control and Collection. Lastly, we asked participants about their demographics: gender, age, education, income, household size, marital status and occupation.

3.2.3 Data Analysis. We collected a total of 495 responses. We inspected the responses and discarded 9 responses because the open-ended responses were simple copy-paste from the Internet, did not contain meaningful responses, or contained numeric entries only. Open-ended questions were used for quality checking and not included in the data analysis. We examined the responses from participants who missed the attention-check questions and discarded all 46 responses that missed one or both attention-check questions.

Consequently, we included 440 responses in our analysis. We performed quantitative analyses on the resulting data. We applied descriptive statistics on participant demographics, SHD types, number of SHDs, privacy control expectations and IUIPC scale items. We performed reliability analysis on the privacy controls categories using Cronbach's alpha reliability coefficient.

3.2.4 Participants. Participants were recruited using MTurk [8]. Participants were located in the US, had HIT approval rating of at least 95%, and had completed at least 100 HITs. Research shows that

[7] https://en.wikipedia.org/w/index.php?title=Smart_home

[8] mturk.com

MTurk population is mostly college graduate. Past reports show that SH users in the US are mostly college graduate, young males [5]. Our participant pool also reflects these characteristics probably because we have included only SHD users in our survey. We provide a summary of participant demographics below.

Gender Identity and Age. 39.1% identified as female, 60.7% male, and 0.2% preferred not to disclose. Mean age was 38.2 years with a median of 35 and standard deviation of 10.5. About 8.6% were 18-25 years old, 42.5% were 26-35 years-old, 26.8% were 36-45 years-old, 14.1% were 46-55 years old, and 8% were above 55 years old.

Education and Income. 62.5% of participants reported having a Bachelor's degree, followed by master's degree (24.5%), some college but no degree (7%), associate (2.7%), high school (2.5%), professional (0.5%) and less than high school (0.2%). 19.3% of participants reported earning no more than $30K, 43.2% no more than $60K, 25.4% no more than $90K, and 12.1% over $90k.

Household Size and Marital Status. The average household size was 3.45 (Mdn=4, SD=1.17). 81.6% reported being married, 15.2% never married, 2% divorced, and 1.1% widowed.

Occupation. Participants reported a diverse set of occupations, including manufacturing, sales, teaching, legal, software development, insurance, software engineering, web design, nursing and accountant. 13% of respondents provided a computer or IT-related occupation.

Device Ownership and Usage. The average number of devices used by participants was 4.76 (Mdn=4, SD=5.04). Similarly, the average number of devices owned by participants was 4.29 (Mdn=4, SD=3.59). The most popular type of device owned and used was a voice assistant, followed by security cameras.

IUIPC Scores. We added up the score for the responses to the questions within each corresponding dimension. The average Awareness score was 15.5 (Mdn=15, SD=3.56, Min=6, Max=21). The average Control score was 15.4 (Mdn=15, SD=3.24, Min=6, Max=21). The average Collection score was 20 (Mdn=20, SD=4.56, Min=6, Max=28).

4 RESULTS

In this section, we describe the results of our qualitative and quantitative analyses. First we will describe the SHD privacy controls desired by the interview participants. Then, we will describe the quantitative insights gained from the survey participants.

4.1 Desired Privacy Controls in SHDs

In this section, we describe the privacy controls expected by our interview participants. The thematic analysis resulted in 215 codes, which were grouped into 30 sub-categories and 7 categories. The codes are the privacy control expectations of users, which are coded as user interface features. The categories and sub-categories inform the design factors and sub-factors respectively.

Thus, we categorized the participants' expectations of privacy controls into seven design factors: Data-related Controls, Transparency, Centralized Interface, Device Controls, Multi-user Controls, User Support, and Security Controls. Table 2 lists the design factors in order of frequency of codes in each category. We describe each design factor in this section, provide participant quote examples for each design factor in Table 3, and provide a listing of all design factors, sub-factors and design recommendations in Appendix A.

4.1.1 Data-related Controls. Most participants (22/25) expressed that they would like SHDs to provide options regarding controlling data collection, transmission, storage and usage. About 40% (n=85) codes fell in this category. By observing the variation in concepts in data-related controls, we divided participants' data control expectations into ten sub-categories: Choice (11%, n=24),

Table 2. Privacy controls categories from thematic analysis of interviews.

Privacy Controls	%	n=215
Data-related Controls	39.5	85
Transparency	19.5	42
Centralized Interface	16.3	35
Device Controls	13.0	28
Multi-user Controls	5.1	11
User Support	3.3	7
Security Controls	3.3	7

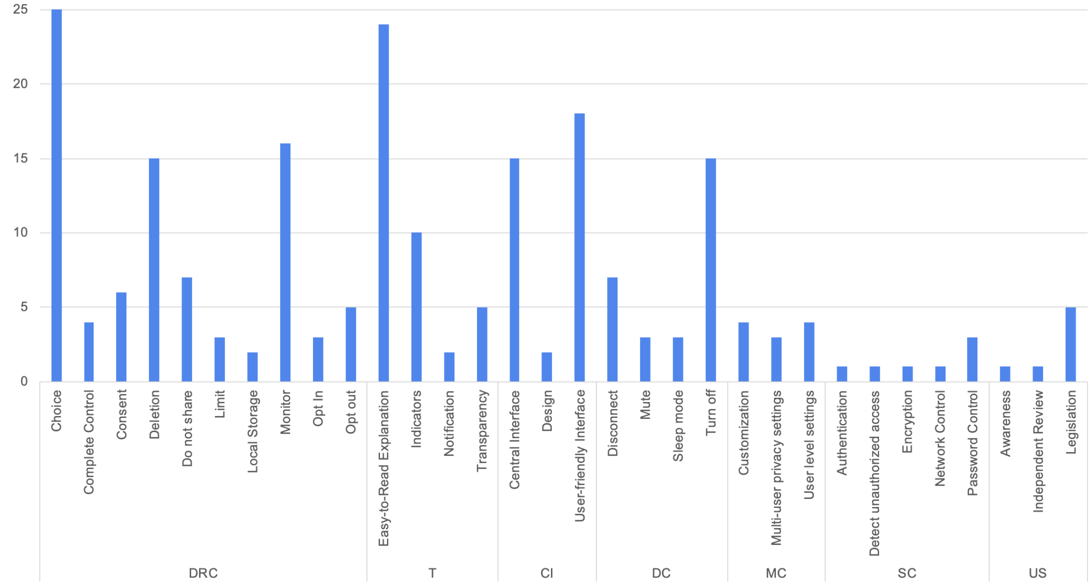


Fig. 2. Design factors and sub-factors with their frequencies (n=215). DRC: Data-related Controls, T: Transparency, CI: Centralized Interface, DC: Device Controls, MC: Multi-user Controls, SC: Security Controls, US: User Support.

Monitor (7%, n=16), Deletion (7%, n=14), Do not share (4%, n=8), Consent (3%, n=6), Opt out (2%, n=5), Complete control (2%, n=4), Opt in (1%, n=3), Limit (1%, n=3), and Local storage (1%, n=2).

Participants whose privacy control expectations fell under the first sub-category 'choice' desired to have options to choose what data are collected by the SHD, what data become part of user profile, what data are shared between devices in a home network, what data are transmitted, what data are shared, what data are used and how. They also sought options for choosing when a SHD records or listens, when data are collected and deleted. Other choices desired included no default social media sharing, option to not make information public, and not storing payment information.

Fourteen participants sought privacy controls that allow them to monitor and audit what data are collected, who they are sent to, and opt in (or out) of data collection. We placed them under sub-category 'monitor'. For instance, one participant highlighted the desire to have options to limit (or not collect) private information:

Table 3. Description of privacy control categories or factors and related sample quotes

Design Factors	Description	Sample Quotes
Data-related Controls	Control over data collection, transmission, processing, storage	“If there is any kind of app or anything that might help me to control the monitoring of data my self and the data being transferred to somewhere else, so I can see like what happened to my data." (P20) “Not collecting a lot of data of private things, more like a cell phone, you know there's not much that can be done about it, so that would be better." (P10) “I don't think there is any way for me to see all the telemetry data that gets sent out to [companies]. If I could basically see, like a telemetry log that I know exactly what they're sending." (P24)
Transparency	Features providing information, policy, disclaimer, indicators showing that device is on and/or in action, and notifications.	"I just think it should be more open about: this is the data we're keeping this is what we throw away. So, mostly I'd like the terms and conditions to just be more straightforward and open about all the privacy." (P23) "If you had [a voice assistant], show a transcript or show whatever you said to it, however that can also give a feeling of less security." (P3)
Centralized Interface	Centralized interface providing smart home device controls.	"Having a centralized area to be able to control where it's very intuitive and I just can turn devices on/off or other things, maybe something like that would be better." (P15)
Device controls	Hardware and software features to control operation of the device or its capabilities, such as powering a device on or off.	"If I could, like, control them from the app and just say, like, stop them all from listening to us at once. Or if I could say to [device] to stop listening. That might already be a thing, but we, I just don't know it. That might be nice, so an easier way than getting up and turning it off." (P8) "Well, I definitely want them to not hear, like each and every word that we say that's definitely the 1st thing I would say, but I don't know how they enable it... may be a sleep mode." (P6)
Multi-user Controls	Controls allowing owners to manage users, their preferences and data	"When I was sharing a smart TV with my parents, if I were watching something on Netflix that I don't want them to see, that would be something that I would be concerned about and I want privacy controls for." (P7)
User Support	Training, Do-it-yourself solutions	"Companies should provide training, ensuring every customer knows how to use the mute button" (P01)
Security Controls	Device security, preventing unauthorized access to the device.	"Mostly, what I want ... is that the information may not be easily leaked. So, what i really want is having the fingerprint and the password, so the company and others cannot access your information." (P18)

> "Not collecting a lot of data of private things, more like a cell phone, you know there's not much that can be done about it, so that would be better." (P10)

Participants who desired monitoring features wanted to audit collected data, view activity, view logs, view audio and video files, and view access logs. For example, a participant who sought monitoring and auditing controls desired options to view what data are collected and what logs are maintained, but mentioned the lack of such features in a current SHD:

> "I don't think there is any way for me to see all the telemetry data that gets sent out to [companies]. If I could basically see, like a telemetry log that I know exactly what they're sending." (P24)

Participants in this category also desired options to delete data. We placed them under subcategory 'deletion'. Automatic deletion of data after a certain period was also a desired feature. Other deletion features included deleting logs (of audio, video), data files one-by-one as well as in large batches, deleting personal information, deleting data after a period authorized by the user, and notifying the user with an option to keep or erase the information.

Participants also expressed benefits of not only providing the choice to the users, but collecting less data. One participant mentioned the lesser the data collected, the lesser the likelihood of damage due to data breaches:

> "I need to be able to see the telemetry data if it gets sent and ideally, it shouldn't be sent on this. There's a good reason to because otherwise that status for all and increases the probability of damage from a data breach." (P24)

We found research evidence connecting secret data collection with data breaches [45]. Another participant who wanted to have control over data desired to have an option of visibility of data transferred and used later:

> "If there is any kind of app or anything that might help me to control the monitoring of data myself and the data being transferred to somewhere else, so I can see like what happened to my data." (P20)

The fourth sub-category included the participants' expectations about 'do not share' features, where participants wanted to be able to not share usage statistics, personal information, and other collected data with the SHD vendor. Two participants also wanted this feature to be default, with an option to share the information when desired.

The fifth sub-category was related to 'consent', where participants desired that SHD vendors asked for the user's consent before: (a) collecting any data, (b) using collected data, (c) transferring those data, (d) sharing data, and (e) updating data.

The sixth sub-category 'Opt out' included five participants who wanted to opt out of data collection that seemed to be lacking in their SHDs.

The seventh sub-category of data-related controls included 'complete control', where four participants desired complete control over their data.

The eighth sub-category 'Opt in' included the needs of three participants who wanted to have data collection opted out by default and wanted that vendors provided options for users to opt in to data collection when the users so wished.

In the ninth sub-category, participants desired options to 'limit' the collection of data, for example, with options to pick what data to allow for collection.

The final sub-category 'local storage' included two participants who sought the option to store and manage data locally in their own home network.

4.1.2 Transparency. About 20% (n=42) of the codes fell under the theme of transparency. In this category, 16 participants desired clarity in SHD companies' data collection and usage policies, clear visual indicators when being recorded, and expected data to be available to review. Participants expected openness from companies in this regard:

> "I just think it should be more open about. Okay, this is the data we're keeping. This is what we throw away. So, mostly I'd like the terms and conditions of things to just be more straightforward and open about all the privacy." (P23)

We divided the codes in this category into four sub-categories: easy-to-read explanation (11%, n=24), indicators (5%, n=10), transparency (2%, n=5), and notification (1%, n=2).

Participants desired an easy-to-read explanation on terms of service, privacy policies, what data are collected, why data are collected, what data are stored and where, how data are used, how long are data retained, what data are shared and under what conditions, with whom data are shared, who has access to data, device capabilities, consent, and benefits and drawbacks of sharing the data, for example if a particular added service would be available by sharing. Among participants who sought transparency on what data is collected, who uses it, and for what reasons, P03 expected options to see transcripts for voice data:

> "If you had [a voice assistant], show a transcript or show whatever you said to it, however that can also give a feeling of less security." (P03)

Another transparency sub-category was indicators. Participants desired to have hardware as well as software indicators for audio recording, video recording, device status (on). Hardware indicator examples include LED lights and software indicators include visible buttons or icons on the user interface.

In addition to indicators, two participants also desired status notifications, such as through voice and visible text display, when SHD is recording audio or video. The term 'transparency' also was used by participants five times.

4.1.3 *Centralized Interface.*

Among all, 15 participants desired a user-friendly, centralized interface that allowed various controls to different smart home devices:

> "Having a centralized area to be able to control where it's very intuitive and I just can turn devices on/off or other things, maybe something like that would be better." (P15)

About 16% (n=35) codes were related to centralized control interface. We categorized them into user-friendly interface (8%, n=18), central interface (7%, n=15), and design (1%, n=2).

Participants desired an interface which is easy to use and provides options to control SHDs in a centralized way. They wanted this interface to be intuitive, child-friendly, elderly-friendly, and mobile. One participant preferred this interface to be voice-activated. Features expected in this central interface included displaying all devices, data practices and disclaimers, viewing data, managing data, visualizing data, and training/tips for the user. Two participants also expressed that the design of the interface should be centered on privacy and focused on the safety of the user.

4.1.4 *Device Controls.*

Participants expressed the need for hardware and software options to turn off the devices and to turn on/off the recording or listening features of the devices. 14/25 participants desired options to isolate or disconnect the device or its recording capability. We divided these device controls into four sub-categories: turn off (7%, n=15), disconnect (3%, n=7), mute (1%, n=3), and sleep mode (1%, n=3).

Participants who desired options to turn off desired capabilities to turn individual devices off, turn all devices off through a button or switch, turn all devices off for a selected period (for example, for a certain period at night), turn listening feature off, and turn recording feature off. For example, one participant, who owned and used multiple intelligent speakers, desired option to turn them off all at once before going to bed:

> "If I could, like, control them from the app and just say, like, stop them all from listening to us at once. Or if I could say to [device] to stop listening. That might already be a thing, but we, I just don't know it. That might be nice, so an easier way than getting up and turning it off." (P8)

Participants desiring 'disconnect' features wanted options to disconnect SHDs from the Internet and wished SHDs asked permission before connecting to a network. Participants also expressed desire for a switch or an option to perform 'hardware disconnect' of a microphone. We learned that hardware disconnect is a feature, similar to one used by Apple[9], where the microphone is disabled in the hardware level so that a malicious software can not invoke the microphone. One participant desired the option to connect SHDs to separate network than the home Internet.

For devices with microphone capabilities, participants wished they had a mute button. Among participants who desired SHDs to not listen to every private conversation, three wished for a 'sleep mode' in SHDs. For example:

> "Well, I definitely want them to not hear each and every word that we say [...], but I don't know how they enable it, may be a sleep mode." (P06)

4.1.5 Multi-user Controls. Seven participants whose desired privacy controls fell in this group sought options for them to customize privacy settings for multiple users. About 5% (n=11) of the codes fell in this category, which included desired features, such as add/remove users, anonymize collected data, optimize privacy settings, do not share (with other users), multi-user privacy settings, option to give permission to family members, schedule SHD operation, display data only for authenticated user, and segregate data by users.

For example, P08 mentioned interest in "curating my own" consumer profile, by editing preferences and interests. Another participant (P07) who desired multi-user privacy settings in a smart television wanted to keep things private from other family members:

> "When I was sharing, like, a smart TV with my parents, if I were watching something on Netflix that I don't want them to see, that would be something that I would be concerned about and I want privacy controls for." (P07)

4.1.6 User Support. Among the participants, 4/25 expressed the need for regulation and third party certification. This category included 3% (n=7) codes: better data rights, legislation on data protection, mandatory deletion requirement, right to delete, user awareness, and independent review/certification of privacy features in SHDs.

Participants desired user training and simplistic design of devices so that users can configure themselves, without the need for professional help. As P01 noted, companies should train their users on privacy features of their SHDs:

> "Companies should provide training, ensuring every customer knows how to use, say, the mute button." (P01)

We also found that participants are finding newer avenues to learn about privacy practices. For instance, P08 expressed having to learn security controls through TikTok videos, such as to control the sharing preferences of usage behavior to not be disclosed with SHD vendor.

4.1.7 Security Controls. This category included 3% (n=7) codes, which were related to user authentication and protecting data from leakage. Six participants' desired features fell in this category, which included options to generate and use password in the SHD, fingerprint authentication, detect unauthorized access to the SHD, control who is allowed to the home network, and data encryption. For instance:

[9] www.apple.com

> "Mostly, what I want regarding privacy is that the information may not be easily leaked. So, what I really want is having the fingerprint and the password, so the company and others cannot access your information." (P18)

4.2 Quantitative Insights on Privacy Controls Desired by Users

From the interviews, we found a number of privacy controls which are desired by users. However, it may be difficult for developers to implement all of them. It is important to know which privacy controls are more important to users. Thus, we present our survey results here to inform which privacy controls were more desired by users. These results may help developers prioritize controls in the implementation. The survey findings may also complement and validate our interview findings.

In Table 4, we show the mean, median and standard deviation of the privacy controls from our survey results in which 440 participants rated whether they wanted a particular privacy control on a scale of 1 (Strongly Disagree) to 5 (Strongly Agree) and we show a graph in Appendix C. The median score for all privacy controls is 4 (Agree) and the average score for most privacy controls is 4 or above, indicating that the privacy controls that were presented to our survey participants were generally desirable. Since the privacy controls that we presented to the survey participants resulted from our interviews, this confirms and validates our privacy controls findings from the interviews.

The top six privacy controls desired in our data set were User-friendly Interface (Mean: 4.25), Access Detection (Mean: 4.21), Indicators (Mean: 4.20), Monitor activity ((Mean: 4.20), Consent (Mean: 4.18), and Independent Review (Mean: 4.18). The least desired privacy control in this data set was Disconnect (Mean: 3.83), probably because the participants assumed they could achieve “disconnect" by simply turning off the SHD.

We tested the scale reliability of our categories using Cronbach's alpha (α) reliability coefficient. We achieved α=0.89 for the category of Data-related Controls, which demonstrated a high internal consistency for the nine items included in it. As shown in table 4, the coefficients for other categories were Transparency-related Controls (α = 0.88), Central Interface (α = 0.69), Device Controls (α = 0.85), Multi-user Controls (α = 0.74), Security Controls (α = 0.83), and User Support (α = 0.68). Similarly, α=0.68 was the lowest scale reliability value obtained, which is considered good for three items. Thus, based on the survey results, our categories demonstrated good internal consistency for the privacy controls items included, as a high coefficient indicates good internal consistency of items in the scale and is dependent on mean of inter-item correlation as well as number of items in the scale [32].

5 DISCUSSION

In this section, we summarize our findings, present recommendations for users and developers, and discuss limitations and suggestions for future research directions.

5.1 Summary of Findings

Our findings suggest seven design factors and 32 sub-factors for privacy controls desired by participants, which were generated from qualitative and quantitative analysis of SHD users' needs. The results presented inform how to design user interface controls for privacy features of SHDs. We also quantified the sub-factors by rigorously designing a questionnaire based on Likert scale. The quantitative insights thus obtained may help developers prioritize controls during implementation.

Since this paper's focus is on the user-centric privacy controls for SHDs, we ensured our codes are semantically formatted in a way that can be translated into a user-interface feature when implemented by a developer. For example, rather than using a code ‘choose', we used the code

Table 4. Mean, median and standard deviation (n=440) of the privacy controls sub-factors from the survey. Mean values below 4 are marked with an asterisk (*), indicating options less desired by survey participants. Scale reliability statistic Cronbach's α values are included in parentheses in the first column.

Categories	Sub-factors	Mean	Median	Std. deviation
Data-related Controls (Cronbach's α = 0.89)	Choice	4.11	4	0.92
	Consent	4.18	4	0.97
	Deletion	4.00	4	1.09
	Do_not_share	3.96*	4	1.03
	Localstorage	4.01	4	0.98
	Limit	4.08	4	0.94
	Monitor	4.2	4	0.98
	Opt_in	4.00	4	0.99
	Opt_out	4.05	4	1.01
Transparency-related Controls (Cronbach's α = 0.88)	Easy_to_read_info	4.15	4	0.87
	Indicators	4.20	4	0.96
	Privacy_policy	4.04	4	0.97
	Notification	4.11	4	1.01
Central Interface (Cronbach's α = 0.69)	Central_interface	4.15	4	0.85
	User_friendly_interface	4.25	4	0.90
	Design	4.16	4	0.95
Device Controls (Cronbach's α = 0.85)	Disconnect	3.83*	4	1.13
	Mute	3.90*	4	1.12
	Sleep	3.86*	4	1.12
	Turn_off	3.92*	4	1.07
Multi-user Controls (Cronbach's α = 0.74)	Multi_user_settings	3.97*	4	0.85
	Maximum_Default_Privacy	4.19	4	0.95
	Customization_User_level	3.96*	4	0.94
	User_level_settings	3.88*	4	1.04
Security Controls (Cronbach's α = 0.83)	Authentication	4.12	4	0.95
	Access_detection	4.21	4	0.91
	Encryption	4.08	4	0.98
	Network_control	4.15	4	0.94
	Password_control	4.14	4	0.92
User Support (Cronbach's α = 0.68)	Training	4.00	4	0.89
	Independent_review	4.18	4	0.96
	Legislation	4.05	4	0.94

'choose what data to delete'. Our paper's unique contribution is this set of privacy controls or codes with granularity and specificity necessary to translate them into user-interface design.

The goal of this paper was to uncover privacy control design factors, sub-factors and privacy-related user interface controls for SHDs comprehensively so that they can be used by developers in user interface design. In the following sub-sections, we discuss our factors and sub-factors in light with prior research, share additional insights gained during analysis, and discuss a privacy control framework and the role of third party or government.

To the best of our knowledge, prior work has uncovered factors and sub-factors of desired privacy features; however, our work extends the knowledge by uncovering user interface controls desired

Table 5. Sub-factors confirmed from prior work and revealed in the current study.

Design factor	Sub-factors from prior work	Sub-factors from this study
Data-related Controls	Deletion [6], Consent [6], Local Storage [6, 70], Limit [71], Choice [70]	Monitor, Do not share, Opt out, Opt in
Transparency	Transparency [6, 35, 70]	Easy-to-read explanation, Indicators, Notification
Centralized Interface	User-friendly interface [70, 74], Design [16]	Central interface
Device Controls	Sleep mode [70]	Turn off, Disconnect, Mute
Multi-user Controls		Multi-user privacy settings, Privacy by default, User level privacy, User level settings
User Support	Awareness [35], Legislation [6, 35, 70]	Independent Review
Security Controls	Password Control [6, 35, 70], Authentication [6, 70], Access detection [70, 74]	Network Control, Encryption

by users in a format that can be translated into design. In order to confirm and extend research in the domain, we used the same names of design factors and sub-factors from prior related work when they existed in prior literature. We now situate our findings with prior work.

5.2 Some Design Factors and Sub-factors Confirm Prior Work

Some of the design factors and sub-factors in this paper confirm findings from prior work. During our thematic analysis, we familiarized ourselves with past literature and used similar terminology when possible. In Table 5, we list the factors and sub-factors revealed from this study and those from prior work on privacy controls of SHDs to the best of our knowledge.

Yao et al. (2019) recommended data transparency and control, safety, and security among six design factors in their paper [70]. Although they did not have sub-factors, we find that some of our sub-factors were included in their work: transparency, delete, multiple users, notice, do not record, and easy interface [70]. Some sub-factors are similar to Barbosa et al. (2020): transparency, access control, consent, security, no data collection, deletion, offline operation [6]. Some of our factors and sub-factors are also similar to the wish list in Haney et al. (2020): transparency (data collection and security feature), security and privacy controls, transparency, and user assistance [35].

5.3 Privacy Controls Contain Usability Heuristics

It should be noted that some privacy control sub-factors contain usability heuristics, which are principles of user interface design [51]. Visibility of system status [51] is a usability heuristic that is contained in our 'visibility' sub-factor. Similarly, Match between system and the real world [51] is a usability heuristic that suggests designers should use language that is familiar to the user (rather than technical jargon) and is contained in the 'easy-to-understand information' sub-factor. In addition, help and documentation [51] is a usability heuristic that is contained in the sub-factor

Table 6. SHD Privacy Control Framework: factors and sub-factors of privacy controls expected by users. Design recommendations, under each sub-factor have been omitted in this table for brevity; they can be found in Appendix A. The 'Where' column defines whether the design recommendations for each factor could be implemented in the SHD itself or its companion app or website.

Design factor	Sub-factor	Where
Data-related Controls	Choice, Deletion, Do not share, Consent, Local Storage, Monitor, Opt out, Limit, Opt in	App, Device
Transparency	Easy-to-read explanation, Indicators, Notification	App, Device, Website
Centralized Interface	User-friendly interface, Central interface	App, Device
Device Controls	Turn off, Disconnect, Mute, Sleep mode	Device, App
Multi-user Controls	Multi-user privacy settings, Privacy by default, User level privacy, User level settings	App, Website
User Support	Awareness, Independent Review	App, Website
Security Controls	Password Control, Access detection, Authentication, Network Control, Encryption	App, Device

'awareness'. Thus, we observe that participants' needs of privacy controls also contain needs of usability.

5.4 Recommendations for Developers: Privacy Controls Framework

The privacy controls that have been uncovered in this paper are ones desired by users. These user expectations can be fulfilled when implemented by developers. In this subsection, we identify the privacy controls that can be implemented by developers. Based on our results, we recommend the following privacy controls framework for developers interested in developing privacy controls in their SHDs. The privacy controls framework consists of the design factors, sub-factors and user interface design recommendations. We list the factors and sub-factors for the privacy control framework in Table 6 and the design recommendations (or user-interface controls/codes) under each sub-factor can be found in the Appendix A. We included all actionable design recommendations from our findings that can be translated into a user interface (UI) feature by developers. For example, we did not include complete data control, because this is a concept rather than a UI item, but included all the choices regarding data control under factor 'choice', e.g. choose what data are shared between devices.

We recognize that the privacy controls desired may be implemented in different elements of the smart home device or network: the SHD device, its app, or SHD vendor's website. For each design factor in Table 6, we also identify the SH component where the privacy controls can be implemented.

The recommendations of our paper can be implemented by developers of individual smart home devices by incorporating them in the design of the device. These recommendations can also be useful to developers of products, such as Fing [10], that are designed to manage smart home devices.

[10] https://www.fing.com/

5.5 Users are Limited to Developer-implemented Controls

SHD users are limited to the privacy controls that are implemented by developers. For example, a user may be interested in viewing what data are collected; however, if that feature was not implemented by the developers, the user would not be able to do so. Thus, the privacy expected by SHD users can come to fruition only when the privacy controls are implemented by developers. Thus, we recommend developers our privacy control framework as a guide towards privacy-related user interface controls and implement features that are feasible in their devices. We recognize that our framework is comprehensive, device-agnostic and flexible, guiding developers to implement privacy controls relevant to their devices.

We recommend that developers not only implement privacy controls discussed in this paper but also make users aware of what privacy controls have been implemented, how users can use these controls, and the implications of these controls to the users.

5.6 Role of Government and Third Party

As prior work has enlightened [35] and some of our participants have articulated, government's role in encouraging some level of privacy preservation could be useful. Participants have expected regulations that ensure privacy of SHD users. The role of government is deemed essential because privacy preservation may not always be in the best interest of manufacturers. For example, limiting collection may be in the best interest of users, but not for manufacturers. Thus, government regulations regarding deletion of personal information, protection of stored data, and proper use of personal information have been expected by participants.

Similarly, an independent, third-party organization could provide verification or certification of privacy features, which would allow novice users the confirmation that the SHD contains the privacy features claimed by the vendor. Displaying certified privacy features could also be beneficial to SHD vendors in gaining the trust of privacy-concerned users.

Although privacy self-management through notice and choice are desirable, the effectiveness of privacy self-management by users is impacted by two factors: (1) the complexity of data collection and usage by highly networked systems, and (2) users' cognitive abilities to make informed decisions by combining the various options picked, choices made, and consents provided. Solove (2012) identified four major problems leading to ineffective privacy self management: uninformed individual, skewed decision-making, scale (of technology), and aggregation [63]. Thus, privacy self-management should be adopted with care, and privacy management should be complemented through other techniques, such as limiting data collection, privacy by design, etc.

5.7 Limitations

The interview participants were mainly young adults, mostly educated, and living in the US. So, typical to any in-depth interview analysis, our results may not be generalizable to populations from other cultures and other parts of the world. The participant pool was not representative and factors such as age, technical proficiency, years owning SHD, education level, nationality, etc. may all affect the results of the study. For example, prior research has shown that age [66] and gender [11] can affect technology adoption. Moreover, the interviews were audio recorded and conducted as a one-on-one conversation, therefore the participants may have felt uncomfortable sharing information that could be embarrassing for them. To minimize the effect, we did not collect any personal information, provided an informed consent according to the approved study protocol, and allowed the use of pseudonyms and cameras to be turned off during interview.

In addition, the recruitment was done online, which may have excluded participants with low digital literacy. The usage of Webex and Miro may also limit the access, so we allowed participants to use their phone to join the interview, in case this approach was more comfortable for them. Thus, our participant population uncovers privacy expectations of early adopters. Finally, our study does not include privacy concerns and expectations of non-adopters of SHDs.

Regarding the survey, the crowdwork platform presents some limitations. As with prior studies using MTurk [6], our MTurk sample is not representative of the US population, but it represents the SHD user population, which is mostly college graduate, young, and technology- or Internet-savvy. MTurk workers also have more information online [39] and likely exhibit privacy concerns not representative of the US public. We also acknowledge that our studies measures users' attitudes, which are known to differ from actual behavior, known as 'privacy paradox' in privacy research [53].

5.8 Future Work

We studied privacy control expectations with participants from the US. Future studies could investigate other populations around the world. Follow up experimental studies could be conducted to validate our findings in other cultural and international contexts. Follow up studies could also develop prototypes and applications to assist developers and users with privacy controls.

We presented a privacy control framework intended to guide SHD developers. Future studies could explore such frameworks for specific devices. For example, a set of privacy guidelines could be devised for camera developers and users of smart cameras.

6 CONCLUSION

Privacy remains a major concern for mass adoption of SHDs [34]. Researchers and developers need to work towards developing privacy enhancing SHDs to address this issue. To decipher privacy control expectations of users, we conducted in-depth interviews with 25 users and analyzed their responses. We then inductively analyzed participants' expectation of privacy features in SHDs to generate seven design factors and 32 sub-factors that can be translated into user-interface design. We complemented and validated the findings through a survey. Furthermore, we recommended design guidelines for developers through a privacy control framework. Developers may use the recommended framework to incorporate user-centric privacy controls in their SHDs, and users may utilize the developer-implemented privacy controls to manage their privacy in SHDs. The findings and recommendations in this paper contribute to a broader understanding of users' needs of privacy controls and ways to address them.

ACKNOWLEDGMENTS

We are grateful to Susanne Furman, Julie Haney, Yaxing Yao and Andrea Limbargo for their valuable inputs in this work. We thank our anonymous reviewers for their valuable feedback on drafts of this work. We thank participants in our pilots and interviews and the MTurk workers who participated in our study. This research was funded in part by 4-VA, a collaborative partnership for advancing the Commonwealth of Virginia, and Commonwealth Cyber Initiative (CCI). Any opinion, findings, conclusions, and recommendations expressed in this material are those of the authors and do not necessarily reflect the views of our research sponsor.

REFERENCES

[1] Ahmed A Abd El-Latif, Bassem Abd-El-Atty, Wojciech Mazurczyk, Carol Fung, and Salvador E Venegas-Andraca. 2020. Secure data encryption based on quantum walks for 5G Internet of Things scenario. *IEEE Transactions on Network and Service Management* 17, 1 (2020), 118–131.

[2] Mark S Ackerman, Lorrie Faith Cranor, and Joseph Reagle. 1999. Privacy in e-commerce: examining user scenarios and privacy preferences. In *Proceedings of the 1st ACM conference on Electronic commerce.* 1–8.

[3] Alessandro Acquisti and Jens Grossklags. 2005. Privacy and rationality in individual decision making. *IEEE security & privacy* 3, 1 (2005), 26–33.

[4] Eirini Anthi, Lowri Williams, Małgorzata Słowińska, George Theodorakopoulos, and Pete Burnap. 2019. A supervised intrusion detection system for smart home IoT devices. *IEEE Internet of Things Journal* 6, 5 (2019), 9042–9053.

[5] Brooke Auxier. 2019. 5 things to know about Americans and their smart speakers. *Pew Research Center. Retrieved from https://pewrsr.ch/2pDPSDX* (2019).

[6] Natã M. Barbosa, Zhuohao Zhang, and Yang Wang. 2020. Do Privacy and Security Matter to Everyone? Quantifying and Clustering User-Centric Considerations About Smart Home Device Adoption. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, 417–435. https://www.usenix.org/conference/soups2020/presentation/barbosa

[7] Jordi Mongay Batalla, Athanasios Vasilakos, and Mariusz Gajewski. 2017. Secure smart homes: Opportunities and challenges. *ACM Computing Surveys (CSUR)* 50, 5 (2017), 1–32.

[8] France Bélanger and Robert E Crossler. 2011. Privacy in the digital age: a review of information privacy research in information systems. *MIS quarterly* (2011), 1017–1041.

[9] Giles Birchley, Richard Huxtable, Madeleine Murtagh, Ruud Ter Meulen, Peter Flach, and Rachael Gooberman-Hill. 2017. Smart homes, private homes? An empirical study of technology researchers' perceptions of ethical issues in developing smart-home health technologies. *BMC medical ethics* 18, 1 (2017), 1–13.

[10] Graham Bleaney, Matthew Kuzyk, Julian Man, Hossein Mayanloo, and Hamid R Tizhoosh. 2018. Auto-detection of safety issues in baby products. In *International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems*. Springer, 505–516.

[11] Mark Blythe and Andrew Monk. 2002. Notes towards an ethnography of domestic technology. In *Proceedings of the 4th conference on Designing interactive systems: processes, practices, methods, and techniques*. 277–281.

[12] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3 (2006), 77–101. https://doi.org/10.1191/1478088706qp063oa

[13] Joseph Bugeja, Andreas Jacobsson, and Paul Davidsson. 2016. On privacy and security challenges in smart connected homes. In *2016 European Intelligence and Security Informatics Conference (EISIC)*. IEEE, 172–175.

[14] Sara Cannizzaro, Rob Procter, Sinong Ma, and Carsten Maple. 2020. Trust in the smart home: Findings from a nationally representative survey in the UK. *Plos one* 15, 5 (2020), e0231615.

[15] Dieter Carbon and Ute E. Carbon. 2021. Ihre Privacy Box. Mehr Schutz im Internet. https://trutzbox.de/

[16] Ann Cavoukian et al. 2009. Privacy by design: The 7 foundational principles. *Information and privacy commissioner of Ontario, Canada* 5 (2009), 12.

[17] Jiahong Chen, Lilian Edwards, Lachlan Urquhart, and Derek McAuley. 2019. Who is Responsible for Data Processing in Smart Homes? Reconsidering Joint Controllership and the Household Exemption. *Reconsidering Joint Controllership and the Household Exemption (November 18, 2019)* (2019).

[18] Chola Chhetri. 2019. Towards a Smart Home Usable Privacy Framework. In *Conference Companion Publication of the 2019 on Computer Supported Cooperative Work and Social Computing*. 43–46.

[19] Chola Chhetri and Vivian Motti. 2019. Identifying Older Adults' Expectations of Privacy-Preserving Controls for Smart Home Devices. In *CSCW Workshop on Networked Privacy, "Ubiquitous Privacy: Research and Design for Mobile and IoT Platforms"*.

[20] Chola Chhetri and Vivian Motti. 2020. Identifying Vulnerabilities in Security and Privacy of Smart Home Devices. In *National Cyber Summit*. Springer, 211–231.

[21] Chola Chhetri and Vivian Genaro Motti. 2019. Eliciting privacy concerns for smart home devices from a user centered perspective. In *International Conference on Information*. Springer, 91–101.

[22] Eugene Cho, S Shyam Sundar, Saeed Abdullah, and Nasim Motalebi. 2020. Will Deleting History Make Alexa More Trustworthy? Effects of Privacy and Content Customization on User Experience of Smart Speakers. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–13.

[23] Roger Clarke. 1999. Internet privacy concerns confirm the case for intervention. *Commun. ACM* 42, 2 (1999), 60–67.

[24] Jessica Cocco. 2011. Smart home technology for the elderly and the need for regulation. *Pitt. J. Envtl. Pub. Health L.* 6 (2011), 85.

[25] Cynthia Dwork. 2008. Differential privacy: A survey of results. In *International conference on theory and applications of models of computation*. Springer, 1–19.

[26] Serge Egelman, Adrienne Porter Felt, and David Wagner. 2013. Choice architecture and smartphone privacy: There'sa price for that. In *The economics of information security and privacy*. Springer, 211–236.

[27] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. 2019. Exploring How Privacy and Security Factor into IoT Device Purchase Behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. ACM, New York, NY, USA, 534:1—-534:12. https://doi.org/10.1145/3290605.3300764

[28] Michael D Fetters, Leslie A Curry, and John W Creswell. 2013. Achieving integration in mixed methods designs—principles and practices. *Health services research* 48, 6pt2 (2013), 2134–2156.

[29] Alisa Frik and Alexia Gaudeul. 2020. A measure of the implicit value of privacy under risk. *Journal of Consumer Marketing* (2020).

[30] Carol Fung and Yadunandan Pillai. 2020. A Privacy-Aware Collaborative DDoS Defence Network. In *NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium.* IEEE, 1–5.

[31] Dimitris Geneiatakis, Ioannis Kounelis, Ricardo Neisse, Igor Nai-Fovino, Gary Steri, and Gianmarco Baldini. 2017. Security and privacy issues for an IoT based smart home. In *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO).* IEEE, 1292–1297.

[32] Joseph A Gliem and Rosemary R Gliem. 2003. Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for Likert-type scales. Midwest Research-to-Practice Conference in Adult, Continuing, and Community ....

[33] Murray Goulden. 2021. 'Delete the family': platform families and the colonisation of the smart home. *Information, Communication & Society* 24, 7 (2021), 903–920. https://doi.org/10.1080/1369118X.2019.1668454 arXiv:https://doi.org/10.1080/1369118X.2019.1668454

[34] Nadine Guhr, Oliver Werth, Philip Peter Hermann Blacha, and Michael H Breitner. 2020. Privacy concerns in the smart home context. *SN Applied Sciences* 2, 2 (2020), 247.

[35] Julie M. Haney, Susanne M. Furman, and Yasemin Acar. 2020. Smart home security and privacy mitigations: Consumer perceptions, practices, and challenges. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Abbas Moallem (Ed.), Vol. 12210 LNCS. Springer International Publishing, Cham, 393–411. https://doi.org/10.1007/978-3-030-50309-3_26

[36] Gunnar Harboe and Elaine M Huang. 2015. Real-world affinity diagramming practices: Bridging the paper-digital gap. In *Proceedings of the 33rd annual ACM conference on human factors in computing systems.* 95–104.

[37] Danny Yuxing Huang, Noah Apthorpe, Frank Li, Gunes Acar, and Nick Feamster. 2020. IoT Inspector: Crowdsourcing Labeled Network Traffic from Smart Home Devices at Scale. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 4, 2, Article 46 (June 2020), 21 pages. https://doi.org/10.1145/3397333

[38] A Jacobsson and P Davidsson. 2015. Towards a model of privacy and security for smart homes. In *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT).* 727–732. https://doi.org/10.1109/WF-IoT.2015.7389144

[39] Ruogu Kang, Stephanie Brown, Laura Dabbish, and Sara Kiesler. 2014. Privacy attitudes of mechanical turk workers and the us public. In *10th Symposium On Usable Privacy and Security ({SOUPS} 2014).* 37–49.

[40] Mi Jeong Kim, Myung Eun Cho, and Han Jong Jun. 2020. Developing Design Solutions for Smart Homes Through User-Centered Scenarios. *Frontiers in Psychology* 11 (2020), 335.

[41] Martin J Kraemer and Ivan Flechais. 2018. Researching privacy in smart homes: A roadmap of future directions and research methods. (2018).

[42] S A Kumar, T Vealey, and H Srivastava. 2016. Security in Internet of Things: Challenges, Solutions and Future Directions. In *2016 49th Hawaii International Conference on System Sciences (HICSS).* 5772–5781. https://doi.org/10.1109/HICSS.2016.714

[43] H Lin and NW Bergmann. 2016. IoT privacy and security challenges for smart home environments. Information, 7 (3), 44.

[44] Naresh K Malhotra, Sung S Kim, and James Agarwal. 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research* 15, 4 (2004), 336–355.

[45] Congcong Mao. 2019. Privacy Issues in IoT: Privacy concerns in smart home.

[46] Carsten Maple. 2017. Security and privacy in the internet of things. *Journal of Cyber Policy* 2, 2 (2017), 155–184.

[47] Davit Marikyan, Savvas Papagiannidis, and Eleftherios Alamanos. 2019. A systematic review of the smart home literature: A user perspective. *Technological Forecasting and Social Change* 138 (2019), 139–154.

[48] Karola Marky, Sarah Prange, Florian Krell, Max Mühlhäuser, and Florian Alt. 2020. "You just can't know about everything": Privacy Perceptions of Smart Home Visitors. In *19th International Conference on Mobile and Ubiquitous Multimedia.* 83–95.

[49] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. 2017. Privacy expectations and preferences in an IoT world. In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017).* 399–412.

[50] Viswam Nathan, Sudip Paul, Temiloluwa Prioleau, Li Niu, Bobak J Mortazavi, Stephen A Cambone, Ashok Veeraraghavan, Ashutosh Sabharwal, and Roozbeh Jafari. 2018. A survey on smart homes for aging in place: Toward solutions to the specific needs of the elderly. *IEEE Signal Processing Magazine* 35, 5 (2018), 111–119.

[51] Jakob Nielsen. 2005. Ten usability heuristics.

[52] Helen Nissenbaum. 2009. *Privacy in context: Technology, policy, and the integrity of social life.* Stanford University Press.

[53] Patricia A Norberg, Daniel R Horne, and David A Horne. 2007. The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of consumer affairs* 41, 1 (2007), 100–126.

[54] Briony J Oates. 2005. *Researching information systems and computing*. Sage.

[55] Maria Rita Palattella, Mischa Dohler, Alfredo Grieco, Gianluca Rizzo, Johan Torsner, Thomas Engel, and Latif Ladid. 2016. Internet of things in the 5G era: Enablers, architecture, and business models. *IEEE Journal on Selected Areas in Communications* 34, 3 (2016), 510–527.

[56] Policy, Research Group, et al. 2016. The Internet of Things: An introduction to privacy issues with a focus on the retail and home environments. *Office of the Privacy Commissioner of Canada, Feb* (2016).

[57] Sandra Spickard Prettyman, Susanne Furman, Mary Theofanos, and Brian Stanton. 2015. Privacy and security in the brave new world: The use of multiple mental models. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*. Springer, 260–270.

[58] Lee Rainie and Maeve Duggan. [n.d.]. Privacy and Information Sharing. Pew Research Center (2016).

[59] William Seymour, Martin J. Kraemer, Reuben Binns, and Max Van Kleek. 2020. Informing the Design of Privacy-Empowering Tools for the Connected Home *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3313831.3376264

[60] Sabrina Sicari, Alessandra Rizzardi, Daniele Miorandi, and Alberto Coen-Porisini. 2018. Securing the smart home: A real case study. *Internet Technology Letters* 1, 3 (2018), e22.

[61] Daniel J Solove. 2005. A taxonomy of privacy. *U. Pa. L. Rev.* 154 (2005), 477.

[62] Daniel J Solove. 2008. Understanding privacy. (2008).

[63] Daniel J Solove. 2012. Introduction: Privacy self-management and the consent dilemma. *Harv. L. Rev.* 126 (2012), 1880.

[64] Benjamin K Sovacool and Dylan D Furszyfer Del Rio. 2020. Smart home technologies in Europe: A critical review of concepts, benefits, risks and policies. *Renewable and Sustainable Energy Reviews* 120 (2020), 109663.

[65] Dirk van der Linden, Matthew Edwards, Irit Hadar, and Anna Zamansky. 2020. Pets without PETs: on pet owners' under-estimation of privacy concerns in pet wearables. *Proceedings on Privacy Enhancing Technologies* 2020, 1 (2020), 143–164.

[66] Emily A Vogels. 2019. Millennials stand out for their technology use, but older generations also embrace digital life. *Pew Research Center* 9 (2019).

[67] Matt Winkler, Alan S Abrahams, Richard Gruss, and Johnathan P Ehsani. 2016. Toy safety surveillance from online reviews. *Decision support systems* 90 (2016), 23–32.

[68] IDC Worldwide. [n.d.]. Quarterly Smart Home Device Tracker, 29 March 2019.

[69] Heetae Yang, Wonji Lee, and Hwansoo Lee. 2018. IoT smart home adoption: the importance of proper level automation. *Journal of Sensors* 2018 (2018).

[70] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. 2019. Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. ACM, New York, NY, USA, 198:1—-198:12. https://doi.org/10.1145/3290605.3300428

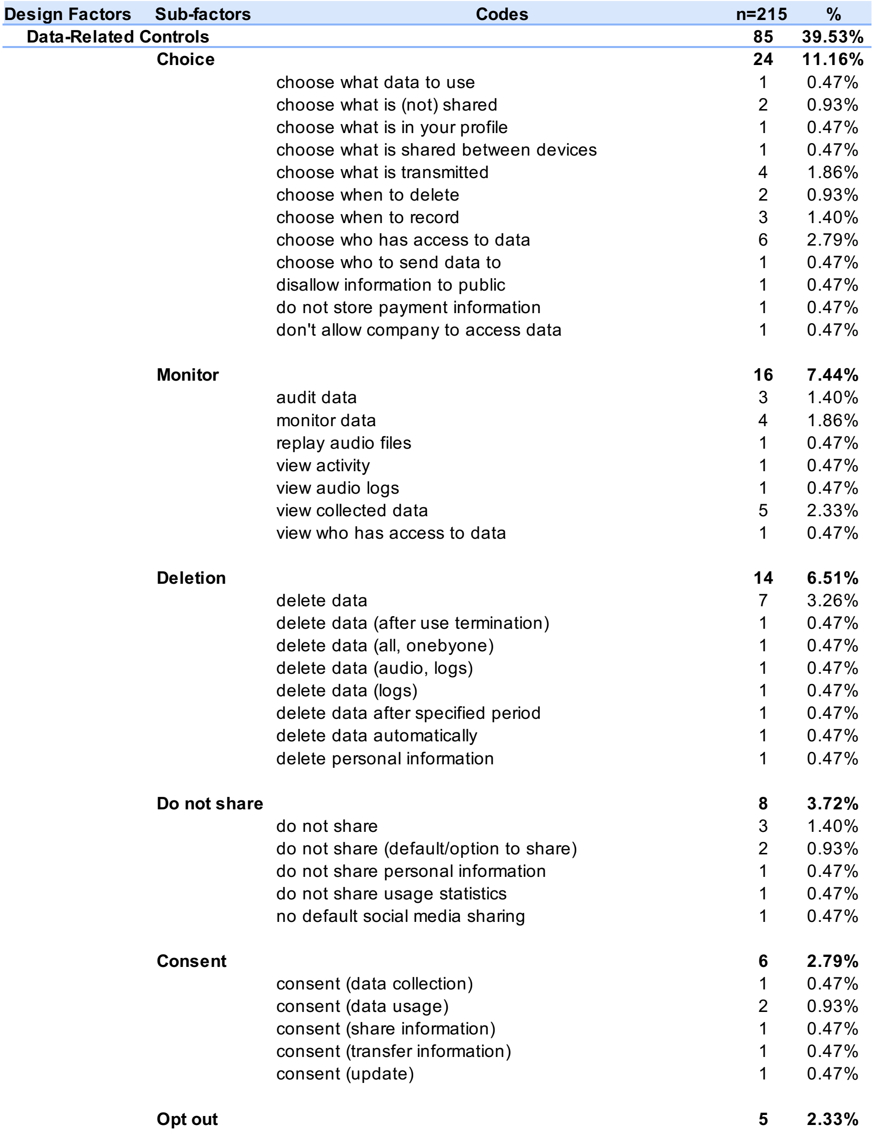
[71] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. 2019. Privacy Perceptions and Designs of Bystanders in Smart Homes. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW (nov 2019). https://doi.org/10.1145/3359161

[72] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End user security and privacy concerns with smart homes. In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*. 65–80.

[73] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User perceptions of smart home IoT privacy. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 1–20.

[74] Verena Zimmermann, Paul Gerber, Karola Marky, Leon Böck, and Florian Kirchbuchner. 2019. Assessing Users' Privacy and Security Concerns of Smart Home Technologies. *i-com* 18, 3 (2019), 197–216.

A PRIVACY CONTROLS CATEGORIES, SUB-CATEGORIES, AND CODES



Design Factors	Sub-factors	Codes	n=215	%
Data-Related Controls			**85**	**39.53%**
	Choice		**24**	**11.16%**
		choose what data to use	1	0.47%
		choose what is (not) shared	2	0.93%
		choose what is in your profile	1	0.47%
		choose what is shared between devices	1	0.47%
		choose what is transmitted	4	1.86%
		choose when to delete	2	0.93%
		choose when to record	3	1.40%
		choose who has access to data	6	2.79%
		choose who to send data to	1	0.47%
		disallow information to public	1	0.47%
		do not store payment information	1	0.47%
		don't allow company to access data	1	0.47%
	Monitor		**16**	**7.44%**
		audit data	3	1.40%
		monitor data	4	1.86%
		replay audio files	1	0.47%
		view activity	1	0.47%
		view audio logs	1	0.47%
		view collected data	5	2.33%
		view who has access to data	1	0.47%
	Deletion		**14**	**6.51%**
		delete data	7	3.26%
		delete data (after use termination)	1	0.47%
		delete data (all, onebyone)	1	0.47%
		delete data (audio, logs)	1	0.47%
		delete data (logs)	1	0.47%
		delete data after specified period	1	0.47%
		delete data automatically	1	0.47%
		delete personal information	1	0.47%
	Do not share		**8**	**3.72%**
		do not share	3	1.40%
		do not share (default/option to share)	2	0.93%
		do not share personal information	1	0.47%
		do not share usage statistics	1	0.47%
		no default social media sharing	1	0.47%
	Consent		**6**	**2.79%**
		consent (data collection)	1	0.47%
		consent (data usage)	2	0.93%
		consent (share information)	1	0.47%
		consent (transfer information)	1	0.47%
		consent (update)	1	0.47%
	Opt out		**5**	**2.33%**

		opt out	5	2.33%
	Complete control		**4**	**1.86%**
		complete data control	4	1.86%
	Opt in		**3**	**1.40%**
		opt out (default)	3	1.40%
	Limit		**3**	**1.40%**
		limit data collection	2	0.93%
		turn off sharing (health data)	1	0.47%
	Local storage		**2**	**0.93%**
		manage data	1	0.47%
		option to store data locally	1	0.47%
Transparency			**42**	**19.5%**
	Easy-to-Read explanation		**24**	**11.2%**
		clear terms and privacy policies	2	0.9%
		clear terms of service/privacy policies	1	0.5%
		disclaimer (what data are collected)	1	0.5%
		easy to read explanation: consent	2	0.9%
		easy to read explanation: data purpose	1	0.5%
		easy to read explanation: retention period	1	0.5%
		easy to read explanation: type of data collected	1	0.5%
		easy to read terms	3	1.4%
		information on device capabilities	1	0.5%
		information on how data will be protected	1	0.47%
		easy to read explanation: how data will be used	4	1.86%
		easy to read explanation: what data will be collected	3	1.40%
		easy to read explanation: how will data be used	1	0.47%
		easy to read explanation: what data will be stored	1	0.47%
		information on benefits and drawbacks of sharing data	1	0.47%
	Indicators		**10**	**4.7%**
		indicator (audio)	1	0.5%
		indicator (listening)	2	0.9%
		indicator (on)	1	0.5%
		indicator (recording)	2	0.9%
		indicator (video)	1	0.5%
		Indicators	1	0.5%
		indicators (alarms)	1	0.5%
		indicators (LED, device status)	1	0.47%
	Transparency		**5**	**2.3%**
		transparency	5	2.3%
	Notification		**3**	**1.4%**
		notification; option to keep/erase	1	0.47%
		notification/awareness when data are used	1	0.5%
		status notification (audio/video)	1	0.5%

Centralized Interface			**35**	**16.3%**
	User-friendly Interface		**18**	**8.4%**
		ADA friendly interfaces (for children and elderly)	1	0.5%
		child friendly interface	1	0.5%
		easy access	2	0.9%
		easy basic and advanced controls	1	0.5%
		easy interface	6	2.8%
		intuitive controls	1	0.5%
		mobile interface	1	0.5%
		quick controls	1	0.5%
		reduce user burden	1	0.5%
		user friendly app	1	0.5%
		voice activation	1	0.5%
		do-it-yourself interface	1	0.47%
	Central interface		**15**	**7.0%**
		app displaying all devices and data	2	0.9%
		automation	1	0.5%
		central control for all devices	1	0.5%
		centralized control interface	3	1.4%
		centralized privacy interface	1	0.5%
		interface showing how the data is used	1	0.5%
		interface showing what data is collected	1	0.5%
		open source friendly	1	0.5%
		privacy-centric design	1	0.5%
		report of collected data	1	0.5%
		standard privacy control system	1	0.5%
		visualize data	1	0.5%
	Design		**2**	**0.9%**
		privacy-centric design	1	0.5%
		safety-focused design	1	0.5%
Device Controls			**28**	**13.0%**
	Turn off		**15**	**7.0%**
		turn all devices off	4	1.9%
		turn all devices off (for specified period)	1	0.5%
		turn off recording /listening	4	1.9%
		turn specific device off	6	2.8%
	Disconnect		**7**	**3.3%**
		disconnect from Internet	4	1.9%
		hardware disconnect	1	0.5%
		permission to connect	1	0.5%
		separate home network	1	0.5%
	Mute		**3**	**1.4%**
		mute	3	1.4%
	Sleep mode		**3**	**1.4%**
		sleep mode	3	1.4%

Multi-user Controls			**11**	**5.1%**
	User-level settings		**4**	**1.9%**
		add/remove users	1	0.5%
		do not share (with other users)	1	0.5%
		option to give permission to family members	1	0.5%
		user-level data display	1	0.5%
	User-level privacy		**3**	**1.4%**
		anonymize	1	0.5%
		customizing privacy settings	1	0.5%
		scheduled operation	1	0.5%
	Multi-user privacy settings		**3**	**1.4%**
		multi-user privacy settings	3	1.4%
	Privacy By Default		**1**	**0.5%**
		default privacy optimized	1	0.5%
Security Controls			**7**	**3.3%**
	Password control		**3**	**1.4%**
		generate secure passwords	1	0.5%
		password	2	0.9%
	Access Detection		**1**	**0.5%**
		option to detect unauthorized access	1	0.5%
	Authentication		**1**	**0.5%**
		fingerprint/password authentication	1	0.5%
	Network control		**1**	**0.5%**
		choose who is allowed to network	1	0.5%
	Encryption		**1**	**0.5%**
		encrypt data	1	0.5%
User Support			**7**	**3.3%**
	Legislation		**5**	**2.33%**
		better data rights	1	0.47%
		legislation on companies	1	0.47%
		mandatory deletion	1	0.47%
		neutral Law	1	0.47%
		right to delete	1	0.47%
	Awareness		**1**	**0.47%**
		user training	1	0.47%
	Independent review		**1**	**0.47%**
		display 'certified privacy' status	1	0.47%

B SURVEY QUESTIONS

(1) Smart home involves the control and automation of home appliances such as washer/dryers, ovens or refrigerators/freezers as well as lighting, ventilation, air conditioning (HVAC), heating (such as smart thermostats), and security. When connected with the Internet, smart home devices are an important constituent of the Internet of Things ("IoT"). The user interface for control of these devices uses wall-mounted terminals, tablet or desktop computers, mobile phone application, or Web interface that may also be accessible through the Internet.
Below you can see example diagrams of three smart home devices: *(Pictures of Amazon Echo, Nest Doorbell, and Smart TV were shown).*

(2) From the given pictures, select the pictures of smart home devices. Please select all that apply. *(Options included pictures of a Nikon SLR camera, Nest learning thermostat, standard Philips blender, Google Home smart speaker, Philips Hue smart light bulb and hub).*

(3) Do you currently use a smart home device? [Yes/No]

(4) *(If "Yes" selected in 3)* What smart home devices do you use? Please check all that apply.
- Security camera
- Doorbell camera
- Baby monitor
- Pet technology
- Motion sensor
- Smoke detector
- Leak sensor
- Smart lock
- Door/window alarm
- Garage door
- Smart light
- Switch/plug
- Voice assistant
- Audio/speakers
- Thermostat
- Smart/automation hub
- Other (Please specify)

(5) *(If "Yes" selected in 3)* How many smart home devices do you use? (Please specify)

(6) *(If "Yes" selected in 3)* For how long have you used smart home devices?
- <1 year
- 1-2 years
- 3-5 years
- 5+ years

(7) Do you currently own a smart home device? [Yes/No]

(8) *(If "Yes" selected in 7)* What smart home devices do you own? Please check all that apply.
- Security camera
- Doorbell camera
- Baby monitor
- Pet technology
- Motion sensor
- Smoke detector
- Leak sensor
- Smart lock

- Door/window alarm
- Garage door
- Smart light
- Switch/plug
- Voice assistant
- Audio/speakers
- Thermostat
- Smart/automation hub
- Other (Please specify)

(9) *(If "Yes" selected in 7)* How many smart home devices do you own? (Please specify)

(10) *(If "Yes" selected in 7)* For how long have you owned smart home devices?
- <1 year
- 1-2 years
- 3-5 years
- 5+ years

(11) *(Open-ended question)* What privacy concerns do you have regarding smart home devices, if any? Provide as much detail as possible.

(12) *(Open-ended question)* What actions do you take to address the privacy concerns regarding smart home devices?

(13) In an app for users of smart home devices, what features would you like to manage your privacy? Select all that apply.
- Manage data collection, use and sharing
- View privacy policy, terms and related information
- Control smart home devices, such as turning them off
- Monitoring data and opting in or out
- Manage multiple users and their accounts
- Learn about features and their implications
- Secure the devices with password and other features
- Other (Please specify)

(In questions 14-21, words capitalized and in parentheses represent the sub-factors and were not shown to participants.)

(14) *(Five-point Likert options from Strongly Disagree to Strongly Agree)* From the following, select your level of agreement with the options you want in smart home devices:
- To choose what data is collected, used and shared. (CHOICE)
- To provide consent for any data collection, use and sharing (CONSENT)
- To delete collected data, audio and video files. (DELETION)
- To not share information about me and how I use my smart home device. (DO NOT SHARE)
- To store data locally in my device or my home network and not in the cloud. (LOCAL STORAGE)

(15) *(Five-point Likert options from Strongly Disagree to Strongly Agree)* From the following, select your level of agreement with the options you want in smart home devices:
- I want to have information on device capabilities, what data is collected, and how is is protected and shared. (INFO)
- I want to see and know when smart home device is recording and collecting data. (INDICATOR)
- I want to see an easy-to-read explanation of privacy policy of the company. (PRIVACY POLICY)
- I want to be notified when my personal information is used. (NOTIFICATION)

(16) *(Five-point Likert options from Strongly Disagree to Strongly Agree)* From the following, select your level of agreement with the options you want in smart home devices:
- Disconnect the device from the Internet. (DISCONNECT)
- Mute my device. (MUTE)
- Put my device to sleep. (SLEEP)
- Turn off all devices at once. (TURN OFF)
- *(Attention Check Question)* Paying attention to the survey. Please select 'Somewhat disagree' to this option.

(17) *(Five-point Likert options from Strongly Disagree to Strongly Agree)* From the following, select your level of agreement with the options you want in smart home devices:
- To limit what data is collected. (LIMIT)
- To monitor what data is collected. (MONITOR)
- By default no data should be collected. I want to sign up for data collection when needed. (OPT IN)
- I want to stop data collection when needed. (OPT OUT)

(18) *(Five-point Likert options from Strongly Disagree to Strongly Agree)* From the following, select your level of agreement with the options you want in smart home devices:
- To create and manage multiple users in my home network. (MULTI USER SETTINGS)
- Default settings should maximize privacy. (PRIVACY BY DEFAULT)
- One users data are not seen by other users of my home network. (USER LEVEL PRIVACY)
- Each user to set their own privacy settings. (USER LEVEL SETTINGS)

(19) *(Five-point Likert options from Strongly Disagree to Strongly Agree)* From the following, select your level of agreement with the options you want in smart home devices:
- Tips and training on how to use the smart home device. (TRAINING)
- To know if an independent third party company has reviewed and certified the privacy features of the device. (INDEPENDENT REVIEW)
- Government regulation requiring protection of data and privacy. (LEGISLATION)

(20) *(Five-point Likert options from Strongly Disagree to Strongly Agree)* From the following, select your level of agreement with the options you want in smart home devices:
- Central control for all my home devices. (CENTRAL INTERFACE)
- Easy-to-use and intuitive features (USER-FRIENDLY INTERFACE)
- By design, it should provide maximum privacy and security (DESIGN)
- *(Attention Check Question)* Select 'Somewhat agree' to let us know that you are paying attention.

(21) *(Five-point Likert options from Strongly Disagree to Strongly Agree)* From the following, select your level of agreement with the options you want in smart home devices:
- Setup password or other authentication such as fingerprint. (AUTHENTICATION)
- Notify me when some one accesses my device or its data. (ACCESS DETECTION)
- Data are protected by encryption or other data protection techniques. (ENCRYPTION)
- Choose who is allowed access to my device and its data. (NETWORK CONTROL)
- Generate secure passwords. (PASSWORDS)

(22) *(Open-ended question)* Think about any additional privacy features that you want in a smart home device (or app). Type them below in the box below as much detail as possible.

(23) *(IUIPC Scale [44], Seven-point Likert options from Strongly Disagree to Strongly Agree)* Please rate your level of agreement with the following statements:
- Consumer online privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used and shared.
- Consumer control of personal information lies at the heart of consumer privacy.

- I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.
- Companies seeking information online should disclose the way the data are collected, processed, and used.
- A good consumer online privacy policy should have a clear and conspicuous disclosure.
- It is very important to me that I am aware and knowledgeable about how my personal information will be used.
- It usually bothers me when online companies ask me for personal information.
- When online companies ask me for personal information, I sometimes think twice before providing it.
- It bothers me to give personal information to so many online companies.
- I'm concerned that online companies are collecting too much personal information about me.

(24) What is your gender?
- Male
- Female
- Non-binary / third gender
- Prefer not to respond

(25) What is your age? (Please specify)

(26) Do you live in the US? [Yes/No]

(27) How many hours do you spend using the Internet every week? [Slider: 0-168 hours per week]

(28) *(Open-ended question)* What is your occupation?

(29) What is the highest level of school you have completed or the highest degree you have received?
- Less than high school degree
- High school graduate (high school diploma or equivalent including GED)
- Some college but not degree
- Associate degree in college (2-year)
- Bachelor's degree (4-year)
- Master's degree
- Doctoral degree
- Professional degree (JD, MD)

(30) Information about income is very important to understand. Please indicate the answer that includes your entire household income in (previous year) before taxes.
- Less than $10,000
- $10,000 - $19,999
- $20,000 - $29,999
- $30,000 - $39,999
- $40,000 - $49,999
- $50,000 - $59,999
- $60,000 - $69,999
- $70,000 - $79,999
- $80,000 - $89,999
- $90,000 - $99,999
- $100,000 - $149,999
- More than $150,000

(31) What is the size of your household?
- 1

- 2
- 3
- 4
- 5
- 6
- 7 or more

(32) Are You now married, widowed, divorced, separated, or never married?
- Married
- Widowed
- Divorced
- Separated
- Never married

(33) Do you have any comments or suggestions for this survey? Thanks

C DIVERGING BAR CHART SHOWING FREQUENCIES OF SUB-FACTORS

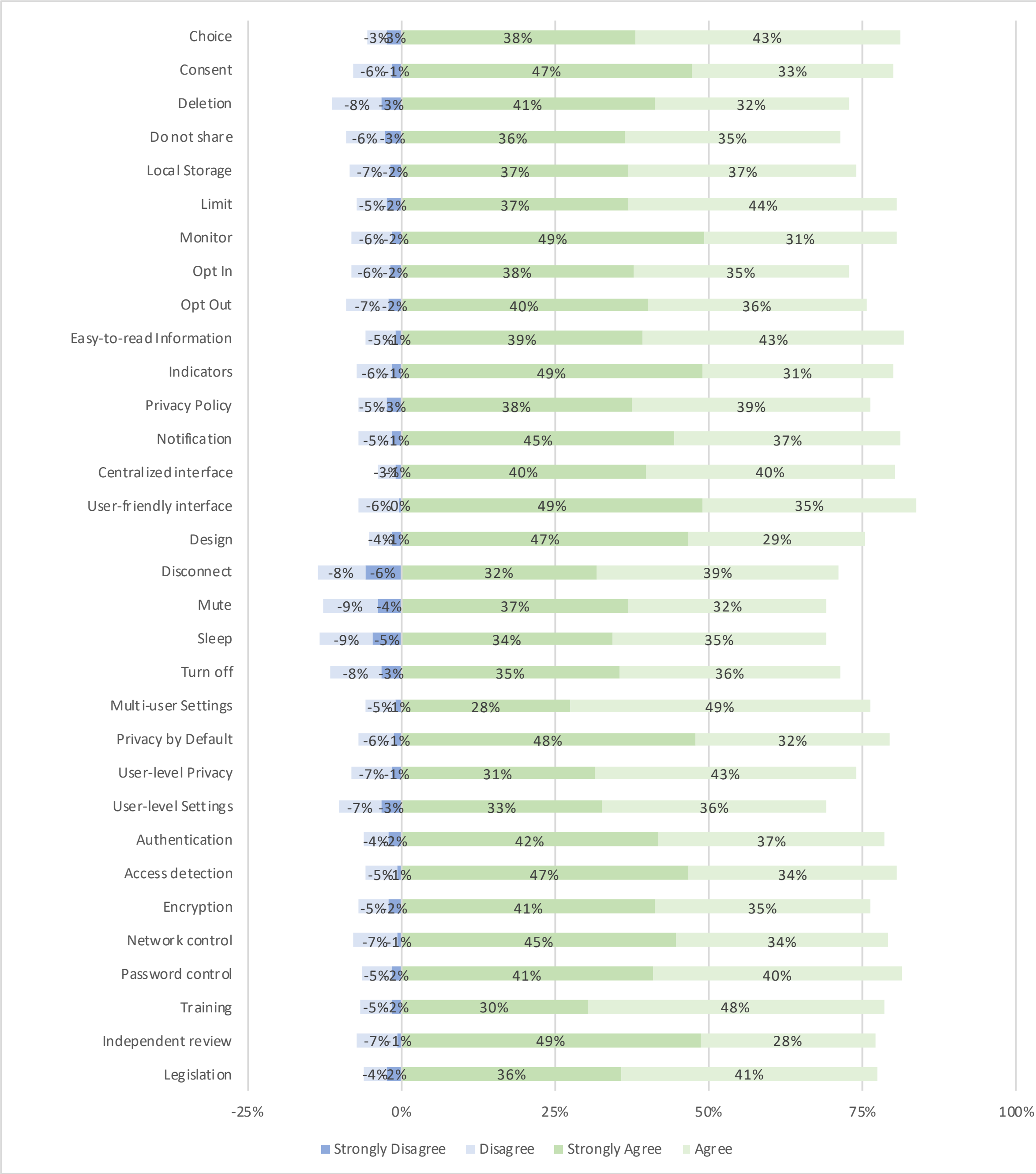


Fig. 3. Frequency breakdown of survey responses for the 32 sub-factors. Neutral responses are not shown.