"Is it always watching? Is it always listening?" Exploring Contextual Privacy and Security Concerns Toward Domestic Social Robots

Henry Bell
Duke University

Jabari Kwesi
Duke University

Hiba Laabadli
Duke University

Pardis Emami-Naeini
Duke University

Abstract

Equipped with artificial intelligence (AI) and advanced sensing capabilities, social robots are gaining interest among consumers in the United States. These robots seem like a natural evolution of traditional smart home devices. However, their extensive data collection capabilities, anthropomorphic features, and capacity to interact with their environment make social robots a more significant security and privacy threat. Increased risks include data linkage, unauthorized data sharing, and the physical safety of users and their homes. It is critical to investigate U.S. users' security and privacy needs and concerns to guide the design of social robots while these devices are still in the early stages of commercialization in the U.S. market. Through 19 semi-structured interviews, we identified significant security and privacy concerns, highlighting the need for transparency, usability, and robust privacy controls to support adoption. For educational applications, participants worried most about misinformation, and in medical use cases, they worried about the reliability of these devices. Participants were also concerned with the data inference that social robots could enable. We found that participants expect tangible privacy controls, indicators of data collection, and context-appropriate functionality.

1 Introduction

Social robots are emerging as the next generation of Internet of Things (IoT) technology [82, 88]. These devices are characterized by their integration of advanced artificial intelligence (AI), physical embodiment, and ability to interact with users on a social level [55, 86]. Social robots are gaining popularity in the United States for the utility they offer in various use cases [16, 32, 107]. They can support users' mental health [120], offer companionship and assistance to patients in medical settings [20, 25, 60], and have been found to be beneficial for educational purposes [83, 93].

Although social robots possess many of the same capabilities as traditional IoT devices, they present unique privacy and security risks to users. To enable their functionality, social robots must collect a massive amount of sensitive and multimodal data from users [114, 115]. The AI-driven interactions of a social robot often prompt users to (over)share sensitive information [128], and if user data is used to train the AI models powering these robots, personal information could be leaked through memorization [9]. Since social robots are more mobile than traditional IoT devices [76], they can create additional threats to users' physical privacy [91] by eavesdropping on conversations [34], or tampering with household objects [34, 112]. Despite these heightened risks, **limited research has examined U.S. users' privacy and security awareness and contextual attitudes toward social robots, particularly within the home environment**.

Prior research, which has emphasized consumer interest in social robots despite their significant privacy and security concerns [77], primarily focuses on social robots within a single context, such as elderly adult [20, 47, 104, 120] or child users [30, 54, 61, 102, 113, 118]. However, in a domestic setting, social robots are likely to engage with multiple users, and fulfill various different needs for each. Each interaction with a social robot presents a nuanced security and privacy landscape that warrants further exploration. This work expands on prior research by examining participants' attitudes, concerns, and expectations towards social robots in multiple scenario-based contexts. It is crucial to form a deep understanding of consumer risk awareness and expectations towards social robots now, while they are still in the early stages of commercialization. The present study addresses this need with three research questions:

- **RQ1:** What level of knowledge and awareness do U.S.-

USENIX Symposium on Usable Privacy and Security (SOUPS) 2025.
August 10–12, 2025, Seattle, WA, United States.

based participants have about domestic social robots and their capabilities?

- **RQ2:** How are U.S.-based participants' security and privacy concerns or comfort levels with domestic social robots informed by different potential use cases?
- **RQ3:** What are U.S.-based participants' security and privacy expectations for domestic social robots in different potential use cases?

Through 19 semi-structured interviews with current users of smart home devices and AI chatbots, we took a critical step toward deepening the understanding of users' privacy needs in relation to domestic social robots. As users of similar technologies, our participants are well-positioned to recognize the dynamic and novel risks associated with social robots in domestic settings. To guide the future development of privacy-aware domestic social robots as they enter the U.S. market, we offer the following contributions:

1. Through an in-depth qualitative analysis, we explore participants' understanding and awareness of risks associated with domestic social robots. Our findings reveal that participants conceptualize domestic social robots through their understanding of similar consumer technologies, such as smart home devices (e.g., smart speakers), and AI-enabled chatbots (e.g., ChatGPT). Additionally, the novelty of social robots makes identifying potential risks difficult for participants. Despite this, many expressed interest in adopting this technology.
2. Our qualitative investigation found that participants' security and privacy concerns and expectations regarding domestic social robots varied widely based on the interaction context. While participants echo many concerns already surfaced in IoT literature, they expressed novel concerns about unique risks of social robots, such as threats to their physical, mental, and social privacy.
3. We surface detailed and context-dependent privacy and security expectations. When used for a medical purpose, participants expected domestic social robots to be regulated under the Health Insurance Portability and Accountability Act (HIPAA); however, they currently are not. In scenarios where a social robot would be interacting with children, participants desired complete control over data collected, preferring the robot to request permission each time it would use data from a child.

2 Background and Related Work

Despite having concerns, people are interested in IoT devices. Prior research has explored individual privacy concerns and mitigation strategies for IoT devices [11, 24]. Zeng et al. [125] found smart home users had fewer security and privacy concerns when they trusted data-collecting entities (e.g., companies or governments) or did not feel personally targeted by advertisements. Emami-Naeini et al. [85] also showed that IoT privacy expectations are heavily influenced by the use context, with participants expressing more comfort when traditional privacy and data protection principles were applied. Despite privacy and security risks, users often prioritize convenience, cost-saving, and connectivity to adopt IoT devices for domestic use: Barbosa et al. [6] found that immediate benefits outweigh privacy concerns for many consumers. However, concerns grow when security-critical devices or ambiguous IoT applications are involved [17, 22, 124]. Trust remains a key factor in user adoption [17, 22, 124], and Emami-Naeini et al. [38] found users are willing to pay premiums for enhanced security.

Users have critical risk misconceptions toward AI chatbots. Chatbots powered by generative AI are designed to interact with users in a human-like way and are adaptable across various applications. Recent chatbots utilize deep learning architectures, including large language models (LLMs), to achieve high levels of performance [1, 126]. They can be used to generate persuasive messaging [62], as an educational tool [58], and to enhance text or produce code [106].

Prior work has established an extensive list of user privacy concerns related to conversational chatbots; these include concerns about data collection, storage, and usage [2, 36, 48, 99, 119], the disclosure of personal information [40, 45, 48, 98], security [51, 64, 79, 87], and transparency [27, 97, 119]. Despite these concerns, users often disclose sensitive personal information to LLMs, even when warned against such disclosures [66]. It has also been well established that people anthropomorphize AI agents [12, 81, 111]. There is evidence to suggest that users disclose more information and better adhere to product recommendations from chatbots perceived as more anthropomorphic [59, 128]. Factors such as visual, conversational, or identity cues of humanness have all been shown to play a role in the anthropomorphism of chatbots [46, 59].

Social robots merge AI chatbots with sensor-heavy IoT devices, yet little research has explored users' concerns and expectations toward these technologies. Recent research has examined the attitudes of different consumers toward social robots. Beer et al. [7] found that demonstrating robot capabilities improved older adults' acceptance of domestic assistive robots. Wada and Shibata [120] examined the long-term interaction effects of the therapeutic seal robot Paro on elderly individuals living in care facilities, reporting that regular social robot interaction could reduce feelings of loneliness and improve mood. Shibata and Wada [104] later demonstrated Paro's positive psychological effects on dementia patients, aligning with Moyle et al. [84], who found it encouraged social engagement.

In parallel with research on older adults, scholars have extensively studied how children interact with social robots in educational contexts. Pioneering work by Kanda et al. [61] introduced a humanoid robot into a Japanese elementary school setting. Over several weeks, children formed social bonds, treating the robot as a peer-like entity. Children remained

positively engaged if the robot's behaviors were socially contingent and responsive. Similarly, Tanaka and Matsuzoe [113] examined how a socially interactive robot influenced foreign language learning in children, observing that children displayed greater willingness to communicate with a robot that offered timely feedback and emotional support. These studies both align with the conclusions of Belpaeme et al. [8], whose review of child-robot interaction literature highlighted the value of personalization, adaptability, and social cues in sustaining children's interest.

However, these technologies also raise privacy concerns. Gao et al. [43] analyzed YouTube and Bilibili reviews to study consumer acceptance of social home robots and found that privacy concerns were a factor influencing user intentions, accounting for 7% of the comments. Another study surveyed U.S. adults (80% of whom were parents) about their perceptions of privacy and attitudes toward social robots in the home [72]. The results indicated that while participants recognized the utility of social robots in public areas such as living rooms, they were more concerned about the risks these devices pose to guests and children, who may be less aware of privacy implications. In a co-learning workshop study by Levinson et al. [73], six families deliberated on allowing social robots to perform various privacy-sensitive tasks. Parents and children negotiated decisions based on specific use cases, highlighting the importance of context and use cases when designing social robots for multi-user home environments.

Our study builds upon existing research on social robots by employing an interview-based approach to surface rich qualitative perspectives on the emerging privacy concerns participants have toward domestic social robots. While prior work has laregely focused on social robot acceptance and trust with specific populations, such as elderly users [20, 35, 120], or parents and children [61, 72, 73], there has been relatively little exploration of security and privacy perceptions toward social robots–particularly across a broader population. In addition, previous research has focused on social robots within specific domains, such as education or elderly assistive care, without systematically comparing concerns across these different applications. In contrast, our study investigates a wider range of use cases, considering contextual factors, user populations, and single vs. multi-use scenarios. By situating our findings within a security- and privacy-centric framework, we explore whether and how these privacy and security concerns align with or diverge from established privacy attitudes of other IoT technologies.

3 Methodology

To surface user privacy and security awareness, concerns, and expectations towards domestic social robots, we conducted 19 semi-structured interviews in March and April of 2024. We recruited U.S.-based participants from the Prolific crowdsourcing platform. No new insights emerged after interview 15, at which point we reached data saturation [100]. Aligned with the guidelines to evaluate the reliability of data saturation, we interviewed 4 more participants [42]. We conducted the interviews online using the Zoom conferencing tool. We presented participants with an informed consent form at the beginning of each interview (see Appendix A.1). Our study protocol was approved by our institution's review board (IRB). We include the interview recruitment and procedure material in the Appendix A.

Participant recruitment. We advertised our study as a research project to understand attitudes toward social robots. We explicitly did not mention privacy, security, or concern in the recruitment message to not prime participants about the goal of this work, mitigating demand characteristic bias [90]. We recruited participants who were at least 18 years old and residing in the U.S.. To increase the quality of the responses, we only recruited Prolific participants with a task approval rating of at least 95%. Prior to inviting the Prolific participants to join our interview study, we administered a screening survey to ask participants about their smart home device ownership, their experience using AI-enabled chatbots, and their demographic background. We then invited a sample of participants who had owned at least one smart home device and had used at least one AI-enabled chatbot. The interviews took, on average, 37 minutes (SD 9.5) to be completed, and participants were offered an incentive of $20 for their participation.

Social robot specification. We designed a specification for a domestic social robot, which has similar capabilities to the social robots on the market. To increase the reliability of the study findings, we told participants that we were independent researchers who were assisting a social robot company in capturing consumers' feedback and opinions on the specifications. This was important to convince participants that the social robot we were discussing was a real device, rather than a hypothetical one. Our IRB office approved this use of deception. After the completion of all interviews, we sent participants a debriefing statement (see Appendix A.4), where we explained the deceptive element and why we used the deception. We also gave participants the option to withdraw their data from being used in the study and raise any concerns with us and the IRB office. No participant expressed concerns or asked to withdraw from the study.

To build the social robot specification, we reviewed the domestic social robots available on Amazon under the searches "Social Robot," "Home Robot," and "Domestic Robot" as of February 2024. We chose these search terms as they are used interchangeably in the existing literature [31, 54, 96] and searched on Amazon since it is the largest e-retailer in the U.S. [3]. For each selected term, we reviewed the search results until the presented products diverged from a domestic social robot. Since our goal was to evaluate participants' attitudes and concerns toward *general-purpose domestic* social robots, we excluded any robot explicitly marketed for a single specific user group (e.g., children), with no

reference of broader domestic use. Our final list consisted of five social robots: EBO X[1], Astro[2], Eilik[3], Misa[4], and Loona[5]. Our goal was to design a *desired* specification with the most comprehensive capabilities. To this end, we compiled a superset of features based on the specifications of the five final social robots. Our specification consisted of six features: 1) `visual recognition`, 2) `voice recognition`, 3) `expressive communication`, 4) `personalization`, 5) `navigation and mapping`, and 6) `internet connection`. The features and descriptions presented to participants are available in Table 2 in the Appendix.

Interview scenario design. We constructed hypothetical scenarios to capture participants' concerns and opinions toward domestic social robots. We walked participants through seven different scenarios, focusing on either the *device recipient* or the *purpose of use*. We considered four levels of `device recipient` which have been shown to impact security and privacy concerns: 1) `purchasing for self` [69], 2) `purchasing for a child` [118], 3) `purchasing for a senior adult` [92], and 4) `purchasing for the household` [65, 109]. For the `purpose of use`, we included three levels: 1) `education`, 2) `medical`, and 3) `psychological therapy`. Prior research has explored the utility of social robots primarily for educational [118], medical [116], and therapy purposes [28, 95]. This is an example scenario that we presented to participants. This scenarios focuses on a `child` as the `device recipient`:

> Imagine that you are living in a family setting with a `child`. You are purchasing this specific social robot for the `child` to be the robot's primary user.

Interview procedure. Our interview consisted of three main sections (see Appendix A.3): 1) knowledge and awareness toward social robots, 2) contextual privacy and security attitudes, and 3) privacy and security expectations toward social robots.

Section 1: Knowledge and Awareness Toward Social Robots. In the second section, we asked questions to gauge participants' current preconceptions and awareness towards social robots. We then presented participants with a working definition for social robots, adapted primarily from the definition found on Wikipedia [122]:

> *"An artificial intelligence (AI) system that is designed to interact with humans and other robots by following social behaviors and rules attached to its role. Like other robots, a social robot is physically embodied."*

We then shared our designed specification (outlined in Table 2) of the prototype social robot with participants, and asked them about their comfort and concern toward the device and its capabilities.

Section 2: Contextual Security and Privacy Attitudes. We then walked interviewees through the social robot scenarios and asked them to explain any specific comfort or concern they have towards each presented scenario.

Section 3: Security and Privacy Expectations Toward Social Robots. Up until this point of the interview, we did not mention privacy or security so as not to bias participants. In this stage of the interview, for the first time, we mentioned security and privacy and asked participants to discuss what features and controls they expect social robots to have to address their concerns.

Qualitative data analysis. We conducted a qualitative analysis of the collected data in two stages. The first stage included an iteration of structural coding where we categorized participants' responses using our three research questions. In the second-cycle coding, we applied thematic analysis [14] to surface the overarching themes and create main codes (e.g., purchase decision factors, expected features of a social robot). All the interviews were coded independently by two researchers on the team. The coders met periodically to jointly create the codebook and resolve any disagreements in the coding. Since the two researchers resolved all disagreements in the codes, inter-rater reliability was not calculated [80]. Due to the qualitative nature and small sample size of our study, we adopt a terminology used in prior work [4, 39, 52, 53] and described in Figure 1 to provide a quantitative representation of the frequency of participant responses.

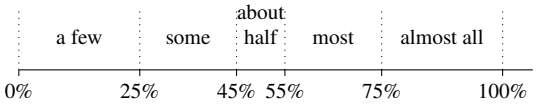

Figure 1: The terminology we use to report participants' percentage in §4. Each term corresponds to a specific percentage range, enhancing the clarity and precision of reporting. For example, "Most participants noted feeling comfortable with domestic social robots." means 55-75% of interviewees reported as such.

3.1 Limitations

As social robots in the U.S. are still in the early stages of commercialization, most participants were unfamiliar with them prior to our interview. Future studies should investigate the concerns of long-term social robot users. Since we used Prolific's pre-screeners to recruit participants, we did not include people who may have used, but not owned, smart home devices. This could have excluded participants who could not afford smart home technology. Additionally, our participant sample consisted mostly of highly educated people, all from

[1] https://www.enabot.com/pages/ebo-x-family-robot-companion
[2] https://www.amazon.com/Introducing-Amazon-Astro/dp/B078NSDFSB
[3] https://store.energizelab.com/products/eilik
[4] https://www.heymisa.com/
[5] https://keyirobot.com/products/loona

the U.S., between the ages of 35 and 54 - there is value in exploring the perspectives of individuals who do not belong to this demographic group. Our discussion of both child and elderly users is only from the perspective of adults, not in either of those groups. The perceived benefits and concerns, specifically for elderly users, could be significantly different from those of adults imagining how an elderly user would use a social robot. To maintain the flow of the interview, we presented the device recipient and purpose of use scenarios sequentially; however, the study could be improved by randomizing the order in which each level and grouping of scenarios was shown to account for order effects [33]. While the factors and levels we investigated in our scenarios are supported by previous research, they are not comprehensive and participants may have had unique concerns in other contexts. A future quantitative exploration could explore a wider range of scenarios and mitigate bias by controlling for the order in which they are presented. Lastly, participant responses could have been biased due to biases associated with self-assessment [63], social desirability [49], and the privacy paradox [127].

4 Results

Our interview sample consisted of 12 female and 7 male participants with an average age of 46. All participants had prior experience with both AI-enabled chatbots and smart home devices. We provide the demographic information of our participants as well as the technologies they have used in Table 1 and Table 3, respectively.

4.1 Knowledge Toward Social Robots

We began our interview by asking participants a few questions to capture their understanding and awareness of the term "social robot." About half of the participants reported no familiarity with the term "social robot". We asked all participants to provide their best interpretation of a social robot. Most participants anchored their definition to an existing digital technology, commonly to available consumer technologies, such as Amazon's Alexa or OpenAI's ChatGPT. This suggests that for individuals for whom social robots are still novel, perceptions of this technology are closely shaped by knowledge of other technologies that share similar capabilities. Most participants defined a social robot as a digital system with capabilities for self-learning, internet connectivity, and social engagement.

The novelty of social robots sometimes made it hard for participants to anticipate the risks associated with them. P17 explained that she wouldn't be able to conceptualize concerns due to her lack of experience:

> I don't know. I wouldn't have any concerns... It's such a new concept. I wouldn't even know where to begin until [I experienced it].

> **Summary of 4.1:** About half of the participants were not familiar with social robots before the interview. These participants tended to conceptualize social robots through their existing understanding of smart home devices and AI-enabled chatbots. Additionally, the novelty of social robots sometimes made it hard for participants to identify potential concerns with the technology.

4.2 Concerns Toward Social Robots

We included six critical and potentially privacy-invasive features of a social robot in our designed specification (see §3). We presented participants with the designed specification and asked them questions to capture their perceptions of the presented capabilities and their concerns toward the described social robot.

Participants were resigned to social robot privacy violations. Some participants explained that while they were not necessarily comfortable with a social robot collecting their data, they viewed it as inevitable, a feeling known as privacy resignation [56]. While P5 expressed discomfort with data collection, they were ultimately resigned to allow it:

> [it's] so terrifying. If somebody laid it all out for me, like, here's everything that Meta knows. Here's everything that Apple and Google know, and how easily they can get that, I'd probably feel uncomfortable. But I think that is part of the social contract that we have with all these companies.

Participants worried about their personal safety. A few participants had concerns surrounding the personal safety threats of a social robot. P14 could imagine how a social robot could be used by others to threaten her safety:

> It shouldn't be abusing and harassing me if I bought it, or serving as a vehicle through which I can be abused and harassed by others

Mobility of the social robot was not a primary concern among participants. Despite these concerns about personal safety, only a few participants expressed concern about the navigation and mapping capabilities of the social robot. While many participants did not focus on mobility as a concern, a few described scenarios where the social robot's mobility would increase the perceived threat of other privacy risks.

P13 explained that her concern that the social robot could collect sensitive information was increased by its navigational capabilities:

> The robot could go around and dig through my purse and look at my credit cards... it could be used for all sorts of things if it's in your home, and it can move around and map.

Participant ID	Gender	Age	Ethnicity	Education
P1	Female	45-54	Hispanic or Latino, or Spanish Origin of any race	Regular high school diploma
P2	Male	25-34	White	Bachelor's degree (e.g., BA, BS)
P3	Female	25-34	White	1 or more years of college credit, no degree
P4	Female	35-44	White	Regular high school diploma
P5	Female	35-44	White	Bachelor's degree (e.g., BA, BS)
P6	Male	55-64	White	Master's degree (e.g., MA, MS, MEng, MEd, MSW, MBA)
P7	Female	45-54	Hispanic or Latino, or Spanish Origin of any race + Brazilian	Bachelor's degree (e.g., BA, BS)
P8	Male	55-64	White	Associate's degree (e.g., AA, AS)
P9	Female	45-54	White	Some college credit, but less than 1 year of college
P10	Male	45-54	Asian + White	Bachelor's degree (e.g., BA, BS)
P11	Male	35-44	Black or African American	Associate's degree (e.g., AA, AS)
P12	Female	55-64	Hispanic or Latino, or Spanish Origin of any race + White	Doctorate degree (e.g., PhD, EdD)
P13	Female	45-54	Hispanic or Latino, or Spanish Origin of any race + White	Doctorate degree (e.g., PhD, EdD)
P14	Female	45-54	White	Doctorate degree (e.g., PhD, EdD)
P15	Male	45-54	White	Bachelor's degree (e.g., BA, BS)
P16	Male	45-54	Hispanic or Latino, or Spanish Origin of any race + White	Associate's degree (e.g., AA, AS)
P17	Female	35-44	White	1 or more years of college credit, no degree
P18	Female	45-54	White	Regular high school diploma
P19	Female	35-44	White	Professional degree beyond bachelor's degree (e.g., MD, DDS, DVM, LLB, JD)

Table 1: Participants' demographic information.

Participants expressed significant concerns toward the passive and active collection of visual and voice data. About half of the participants reported having privacy concerns regarding the audio and video collection of social robots, either being collected as a result of intentional interaction with the device or being passively collected without users' interaction. P5 was concerned about where identifiable information would be stored:

> So as it's doing all this learning… like learning my face, learning my voice. Where is all [the data] being stored?

Similarly, P6 discussed their privacy concerns with being in the presence of a social robot and expressed interest in having information about devices' privacy and security practices:

> What's going on with the data on the back-end? How much of my privacy am I giving up by just being in the environment with that robot?

No participants talked about unique risks introduced by the AI components of social robots. A key example is memorization, where the AI models powering these robots can unintentionally memorize sensitive information during training and potentially expose this data to other users [9].

Participants were not comfortable with data inference. A few participants worried about the information that could be inferred from their interactions with a social robot. P4 described how she was uncomfortable with what Google inferred about her:

> I have actually looked through the data that Google knows about me, and it's a little bit creepy because they know things that I have not directly told them... How did they get that information?

When comparing a social robot to her current smart speaker, P4 explained that data inference from a social robot would be more concerning since it would collect more data:

> [Social robots] could be a little smarter, and that could be a little more concerning, just because, you know, maybe they're inferring even more things... maybe because there would be more information that they would have.

Prior research has shown that the context in which the technology is being used can significantly impact users' security and privacy concerns and perceptions [92, 110]. We presented hypothetical data collection and use scenarios in which a household social robot is being primarily purchased for a `device recipient` (four levels: yourself, children, elderly, household) or to satisfy a `purpose` (three levels: educational, medical, therapy).

Most participants did not worry about scenarios in which they were the primary user of a household social robot. Most respondents expressed little or no privacy or security concerns toward purchasing a social robot for themselves. The most commonly mentioned benefit of having a social robot was companionship. Other frequently mentioned benefits of social robots include safety and productivity. P1 discussed why they were comfortable with purchasing such a robot for themselves:

> It would make me feel safer, if anything were to happen, I'm sure I could ask it to dial 911.

When imagining purchasing a social robot for themselves, a few participants reported having concerns about the data practices of the device. One participant in particular worried that their sensitive information could be used against them:

> I think the most uncomfortable aspect of it is like, how much does it know about me? Can that information be used by somebody else, and can it be used against me in any way?

One expected use of a social robot in this scenario was to monitor relevant household items. P6 explained that a social robot would be beneficial for reminding him about the needs of his dog:

> I'm not necessarily gonna ask it to fill the water bowl, but at least inform me. 'Hey no, he needs this, or it looks like he's low on treats, or it looks like he wants to go out', so I don't constantly have to be like getting up and doing those kinds of things.

Most participants were concerned about their children interacting with household social robots. Most participants mentioned at least one privacy or security concern with a child being the primary user of a household social robot. There were significant concerns surrounding children's data security and privacy, and social development. P9 discussed their significant concerns about their kids' natural behaviors being recorded by a social robot:

> The visual thing would bother me with [my daughter] being a child. I've had to be careful with her... that she's not trying to get changed or anything.

A few participants imagined a social robot being used to help their child complete chores. P14 expected the robot to remind their child to stay on task, and to help with some chores:

> If it could assist the child with their homework, or their tap their list of chores, or remind them to be doing things they need to be doing instead of Mom and Dad having to be that person [that would be] helpful... could it clean their room, or, you know, fold their laundry?

While some participants mentioned companionship as a potential benefit of allowing a child to interact with a social robot, a few participants worried that this "artificial" socialization would have negative impacts on their children's development. P5 explained that she would prefer her children to interact with other children, rather than a social robot:

> I wouldn't buy my kid a robot friend. I would encourage my child to have social relationships with actual human children. I just don't think that is something I would layer in as an experience for my kid.

A few participants worried that children might misuse the device to access age-inappropriate content online, or make purchases without informing their parents. P4 was particularly concerned about this:

> [I] also have concerns with the child accidentally buying things, or signing up for [subscriptions] that would cost money.

Despite concerns toward being deceived, the perceived benefits of domestic social robots for senior adults outweighed the potential privacy harms. Most participants were comfortable with purchasing a social robot for an elderly family member. It is important to note, however, that most of our participants are under the age of 65 and would not be considered elderly. These participants often discussed the purchase of a social robot for their own elderly parents. This should be kept in mind when interpreting the results, as elderly users may feel differently if asked to purchase this robot for themselves [70, 74]. About half of the participants reported that a social robot would be beneficial in providing companionship for elderly family members. Assisting with medical care needs for senior adults was the second most frequently perceived benefit of social robots. Some participants felt that a social robot could bring them peace of mind. P6 described specifically how this could be a benefit:

> I could definitely see [the robot] as being a really good watchdog, so that if anything happened with my mother, we would receive some sort of a notification.

Lack of usability was the most frequent concern when discussing elderly users of social robots. About half of the participants worried that the device would not be usable for an elderly user, and that it would be hard to convince an elderly family member to adopt the technology. P13 worried that an elderly user would struggle to use a social robot. A few participants mentioned having privacy and security concerns about senior adults' use of social robots. Our participants were primarily concerned that the robot would influence senior adults to share sensitive information about themselves. P7 said:

> I would want to make sure that their information is safe. Because, especially with the elderly, they don't always know when they're being swindled.

Maintaining confidentiality was the main privacy concern when sharing a social robot with household members. In a communal setting where multiple users would share a social robot, about half of the participants worried about their data being leaked to other users. P14 worried about potential malicious behavior in a shared living setting:

> Is there sensitive information that the other roommate could, if they had ill intention, access?

A few participants mentioned bystander privacy as their main concern with social robots being shared among household members. P2 discussed the importance of ensuring that everyone in the communal setting is comfortable with a social robot:

> I would be comfortable, but it might make [my roommate] a little uncomfortable.

Misinformation was the primary concern in using social robots for education. Participants saw potential educational benefits of using social robots, especially for children. These participants reported that social robots could be useful in helping children with their homework and assisting educators

outside of a classroom setting. P9 described how her child attends school virtually, and so having a social robot to help teach content would be helpful:

> My daughter does cyber school... this is an everyday battle, and I'm like I didn't learn this stuff 30 years ago. So yeah, I would be absolutely comfortable.

Some participants still worried about the reliability of social robots as an educational tool. Misinformation and potential hallucination effects were frequently mentioned. Prior research supports this concern, documenting hallucinated responses to questions across many topics [126]. P19 worried about information accuracy, comparing the social robot to ChatGPT and Alexa:

> I don't know that I would trust it cause I know it could be just like how ChatGPT works or how [Alexa] works. I know sometimes they come up with nonsense.

Lack of reliability was the main concern for using social robots in a medical context. The most common concern participants had about using a social robot in a medical setting was the lack of reliability of the decisions made by the device. Despite this, about half of the participants reported being comfortable using a social robot as part of a larger care plan. P3 saw medical social robots as a starting point for treatment, but not a replacement:

> I think anything like that is open to misinformation, so I would use it as a starting point, but not to replace a doctor.

Some participants worried about the medical data a social robot would collect. P19 explained she would be comfortable with a social robot doing some tasks, but not collecting data:

> [Medical use] is a very wide ranging topic. If it was like reminding me to take pills, or to check my [pulse oxygen] or blood pressure, sure, great! If it was recording any of that info or giving any type of advice, absolutely not.

The use of the social robots for therapy did not introduce new privacy or security concerns. Despite seeing convenience as a benefit, about half of the participants saw social robots as less effective than human therapists. These participants tended to believe that human-to-human interaction was necessary for effective therapy, and expected interacting with a social robot to be shallow in comparison. This belief is similar to the "Perceived Loss of Human Touch" often described with generative AI in medical contexts [105]. P7 mentioned:

> I think it could be very helpful in certain scenarios, but again... is it helping the evaluation process? Or is it helping like a mental health patient who can use support in some way? I feel like that could be a supporting technology, assistive in some ways

A few participants had concerns about how the unreliability of generative AI could harm people seeking psychological help. P19 worried about the impact that inaccurate information could have:

> I don't know the advice [social robots] are giving, and if someone is in a vulnerable state, that could be extremely dangerous and harmful.

Summary of 4.2: Participants' concerns about social robots were shaped by their experiences with smart technologies, focusing on audio and video data collection while overlooking navigational risks. They were least concerned about owning a social robot, but were hesitant about purchasing one for a child. While recognizing benefits for elderly users, they noted usability challenges. Multi-user robots raised concerns about data leakage and bystander privacy. Participants favored low-stakes tasks but opposed replacing human practitioners in critical roles.

4.3 Transparency For Social Robots

Almost all participants expected social robots to provide trustworthy information about their security and data practices through multiple modalities. Aligned with prior work on IoT devices [21, 67, 89], our participants wanted to know what data is being collected and used for, who it is shared with, and how it is protected.

Information about what data is being collected and inferred. About half of our participants reported being interested in knowing what type of information the social robot can collect and learn about them. In addition, participants wanted to be informed about how this information is collected.

Information about the purpose of data collection. About half of the participants expressed interest in knowing what the data collected on them would be used for. Consistent with prior research, participants were more accepting of data collection that personalized the devices or contributed to their functionality [129]. P15 was not comfortable with sensitive data being collected, but was okay with personalization:

> I think this goes without saying [that I don't want the robot] giving personal health data or a bank account data or anything... But there's lots of stuff I don't mind. I mean, if it's personalizing the experience, I don't mind giving up a little bit.

Information about how the data is being protected. Most participants felt that both the social robot manufacturer and the user of a social robot were responsible for maintaining security and privacy. About half of the participants wanted

information on the data protection practices in place. Some wanted to know about the security measures of the device to ensure their robot could not be hacked and used by adversaries to collect data. P18 explained that she would want to know about the safeguards in place, as well as the manufacturer's reputation in securing user data:

> I would want to know what is going on with [my] information. How secure is the company that produces this robot?... How well does it do with security? Does it have a number of breaches? What protocols are put in place to protect sensitive information?... What's the company's track record?

Information about user privacy controls. Some participants wanted control over who could access the device and its collected information. P13 described a scenario in which access control would be valuable for keeping house guests from accessing the social robot:

> Say, for instance, I invite someone over to stay at my house that I may not know completely well, or have a relative come and stay at my house. I don't want them to be able to easily access [the robot]

Information about the models that power the AI functionality of the social robot. When prompted about AI transparency specifically, about half of the participants wanted to have more information about the model powering the conversational AI of a social robot. This included the model that was being used, the data it was trained on, and its ability to adapt and learn from the user. A few participants also mentioned the trustworthiness of the AI.

Providing transparency through multiple channels, including on package and through the device. When asked about the preferred modality of transparency in social robots, most participants reported that they would like the security and privacy information to be presented to them through multiple channels as opposed to one single method. When explaining his preferred method of communication, P10 said:

> In every way. Writing, video, disclaimers... I think clarity is kindness... it's the responsibility of the manufacturer to be upfront with all the possibilities.

Most participants expressed a preference for security and privacy information to be on a device's packaging or to be available online. Participants noted that, while convenient, it might be infeasible to fit all of a device's information onto its physical packaging. P14 explained how she would expect the information to be present on the device's packaging, but would also seek out more details online.

> I think it should be on the box, and I definitely think there should be a website that details the specifics. I [would] probably look on the website honestly.

A few participants reported that they prefer the social robot to communicate its own privacy and security information, expecting the robot to leverage its voice and visual interfaces to convey its security and data practices to the users.

> **Summary of 4.3:** Participant expectations of security and privacy transparency in social robots were similar to expectations towards traditional IoT and smart home technologies. Participants primarily wanted to know what data was being collected, what it was being used for, and who it was being shared with. They also wanted to know about the privacy controls available for social robots and the AI models that power them. Participants expected this information to be available in various modalities such as online, on the device packaging, or through the social robot's communication interface.

4.4 Expectations Toward Social Robots

We asked participants about the features they expect social robots to have to protect their security and privacy.

On-device visual and audio cues to signal data collection and processing. Some participants mentioned that a visual or audio cue that the device was currently collecting data would mitigate some of their privacy and security concerns. P4 worried that they would not be able to tell when a social robot was collecting information:

> Is it always watching? Is it always listening? Is there some sort of cue I would give it that would cause it to listen/see?

Ability to review and delete the collected data. A few participants expected social robots to behave similarly to some smart speakers [69], letting users review and delete the data a social robot collects. When discussing their comfort with the speech recognition capabilities of social robots, P4 said:

> I do make a habit of going in and deleting all of the voice recordings, double checking that it's not hearing things.

Being able to cover device sensors to limit data collection. A few participants expected to be able to cover and/or unplug the sensors on social robots. P14 mentioned that she would want the ability to disable data collection with a physical button on the device:

> [I would want] a kill switch to not have anything be recorded... I'd want to have full control over what information is going out

Parental control to manage data practices of social robot. Parental controls were the most frequently requested feature among participants who reported being concerned about children's use of domestic social robots. Participants wanted to

have control over what data a social robot could collect from their child. P11, for example, preferred the robot to ask for permission before using any visual data of their child:

> Give me an authorization request... like 'are you okay with using your kid's image'?... An authorization to consent to the use of my child's images.

Policies and regulations to control the data practices of social robots. Some of our participants mentioned the need for having strong security and privacy regulations and standards for social robots, especially when being used in sensitive use cases, for example, assisting an elderly household member with their health needs. P7 mentioned:

> We have very strict rules about privacy and medicine. As long as it stays within [HIPAA] I think it could be very helpful.

Unless provided by a covered entity, data collected by household social robots is not protected under health privacy laws, such as the Health Insurance Portability and Accountability Act (HIPAA). This response from participant 7 indicates a lack of awareness of the available regulations to protect users' data when interacting with domestic social robots.

> **Summary of 4.4:** Participant expectations toward security and privacy controls in social robots closely mirrored preferences identified in prior research on smart home devices broadly. Participants wanted clear signals when data collection was happening and tangible controls to disable specific sensors based on the current context of use. They also wanted strict and granular parental controls and the ability to review, collect, and delete all data a social robot collects. Lastly, participants emphasized the importance of strong and clear regulations and standards for social robots.

5 Discussion

Our study contributes to the ongoing discourse on privacy and security concerns surrounding domestic social robots. While prior research has primarily focused on user acceptance and trust [10, 43, 68, 94, 131], our work investigates security and privacy attitudes toward these robots. Additionally, existing studies on social robots, including those addressing security and privacy, often examine predefined use cases such as education or assistive care [7, 20, 35, 61, 113], or focus on specific user groups like children [73] or parents [72]. We explore concerns across multiple use cases, allowing for a comparative analysis of privacy and security risks.

In brief, our findings reveal that most participants were unfamiliar with the term "social robot," yet they consistently associated these devices with self-learning, social engagement, and internet connectivity (See §4.1)–aligning with prior literature [57]. Nearly all participants voiced privacy concerns regarding domestic social robots even before being explicitly prompted (See §4.2), with primary concerns centered around the audio and visual data collection capabilities of these devices (See §4.2). While similar concerns exist for smart home devices [21, 71, 129], our findings suggest that domestic social robots introduce an additional layer of apprehension due to their autonomous interactions; many worried about data collection occurring without their awareness or explicit consent (See §4.2). These concerns were highly context-dependent. Participants generally expressed fewer concerns about personal ownership of domestic social robots but were significantly more cautious about their use by children and the elderly (See §4.2). Consistent with smart home devices studies [92, 110], participants prioritized child privacy and raised concerns about the usability challenges for older adults. Despite prior work suggesting that social robots function best in shared-use scenarios [5, 37], our participants were largely uncomfortable with multi-user interactions due to privacy risks. Finally, despite the AI capabilities of social robots, participants expressed relatively little concern about risks specific to generative AI. This suggest a potential lack of awareness about emerging threats, which may stem from the novelty of these devices and the tendency to associate social robots with traditional IoT devices rather than advanced, evolving, AI systems (See §4.2).

Social robot as an all-in-one smart home. As embodied agents, social robots could potentially replace users' smart home devices as all-in-one home technology. Consolidating the smart home ecosystem in this way could have privacy and security implications for users.

Increased Risk of Data Linkage. One implication of consolidating a smart home into one device is the ease of data linkage [78, 130]. In traditional smart homes, data collected from multiple separate IoT devices is not necessarily linked to a single user. However the multi-modal data collection of a social robot is inherently linked. This linked data can be more revealing of sensitive user information or used to infer information not explicitly provided by the user [130]. Social robot developers should refrain from taking advantage of this linked data, as our participants expressed discomfort with data inference (See §4.2), and expected complete transparency on how their data would be used (See §4.3).

Mitigating Privacy Fatigue Through Centralized Management. Privacy fatigue refers to a sense of weariness toward privacy issues, in which individual believe there is no effective way to manage their private information online [23]. This concept is closely tied to privacy resignation and cynicism, where users feel disempowered and accept pervasive data tracking as an unavoidable reality [56]. Indeed, while almost all of our participants expressed security and privacy concerns before we explicitly raised the topic (See §4.2), some conveyed a sense of resignation, stating that although they were uncomfortable with data tracking, they felt it was inevitable since data collection happens across all digital devices (See §4.2).

As standalone devices, in lieu of an ecosystem of multiple

smart devices, social robots could potentially reduce privacy fatigue by simplifying privacy management. Instead of navigating separate settings for numerous smart home devices, users could configure and monitor their privacy preferences from one place–either because the domestic social robot is the only smart device in their home or because it serves as a personal privacy assistant [29, 117] integrating with and controlling other devices. This could help users manage their privacy more efficiently, reducing their cognitive overload. If social robots are to consolidate information from across users' homes, it is imperative that they align with user security and privacy expectations and allow users fine-grained controls to specify their data-handling preferences. Our participants outlined detailed expectations regarding security and privacy measures in domestic social robots (See §4.4). These include the ability to review, control, and delete their information.

Lack of regulations for social robots. Regulations should proactively anticipate the role of domestic social robots and their impact on user privacy, including their potential function as privacy management tools. Some participants viewed policymakers as the primary stakeholders responsible for protecting consumers privacy. However, there are currently no specific, comprehensive privacy laws governing social robots. Given their extensive sensor data collection, conversational AI capabilities, and anthropomorphic design–which encourages greater user disclosure– [59, 128] we argue that distinguishing social robots from standard IoT devices in legal frameworks is essential. Their ability to function as all-in-one devices further complicates regulatory considerations. For instance, one participant expressed trust in existing privacy regulations for healthcare, assuming that the Health Insurance Portability and Accountability Act (HIPAA) would apply to social robots (See §4.4). This is a common misconception. HIPAA only applies to "covered entities" such as healthcare providers and insurers, excluding non-covered entities like fitness and mental health apps. As it stands, domestic social robots do not fall under HIPAA unless they are provided by a covered entity, even if they help with health-related tasks.

Similarly, the Children's Online Privacy Protection Act (COPPA) presents limitations when applied to social robots. While COPPA restricts the collection of data *from* children under 13—an issue frequently raised by our participants (See §4.2)—it does not regulate data collected *about* them. This loophole allows for the indirect collection of sensitive information *about* children, undermining the law's intended protections. In the case of social robots, a single device may be used by all household members, and, in theory, could collect data *about* children present in the house through its various sensors, without necessarily collecting it directly from them.

The Federal Trade Commission (FTC) has some authority under Section 5 of the FTC Act to address unfair and deceptive trade practices. The FTC has taken action against multiple Tech companies, including a recent crackdown on deceptive AI claims [26]. For example, the FTC has taken action against DoNotPay, a company that falsely advertised an AI service as "the first robot lawyer." [26] However, FTC enforcement is reactive rather than proactive. It relies on consent agreements requiring companies to implement privacy and security measures for up to 20 years, with civil penalties only imposed if they violate these terms. This approach limits the FTC's ability to deter misconduct before harm occurs. Despite some recent promising state-level efforts to regulate AI [50, 123], privacy advocates agree that robotic technology poses challenges to existing privacy laws [19, 41, 47]. AI policies that fail to consider the specific context of robotic applications risk being ineffective [41]. As illustrated by the examples above, existing privacy regulations in the U.S. already fall short in protecting consumers from the privacy and security risks domestic social robots pose.

Several studies have examined the extent to which robots comply with privacy regulations. Horstmann et al. identified privacy concerns in four use cases and proposed a privacy app concept to mitigate GDPR violations [57]. Shcafer et al. advocated for amending the UK's Principle 4 of ethical robot design to include "transparency by design" [101]. Villaronga et al. explored ethical, legal, and societal challenges associated with social robots in healthcare, aligning their recommendations with recent European robotics regulatory initiatives [41]. However, more research is needed specifically within the U.S. regulatory context. Calo laid the groundwork in 2010 by analyzing the privacy risks posed by robots in relation to U.S. regulation [19]. However, both the robotics field and regulatory frameworks have evolved significantly since then. We urge future research to reexamine these issues, as our participants expect policymakers–alongside designers and users–to play a critical role in mitigating privacy risks.

More than just data: the overlooked privacy dimensions of domestic social robots. There is no single definition of privacy that encompasses all of its facets. A common approach in privacy scholarship is to examine privacy through multiple dimensions, each addressing different types of privacy risks and concerns [108]. Security and privacy research in HCI has traditionally focused on informational privacy, which is central to discussions on data collection, storage, and usage–concerns that were prominent among our participants. As we elaborate throughout Section 5, many expected clear disclosures about data handling and desired mechanisms for transparency and control. However, given the defining characteristics of social robots–embodiment, autonomy, and anthropomorphism– it is valuable to examine their privacy implications beyond informational privacy. We discuss physical, psychological, and social privacy as key dimensions that are particularly relevant to social robots. Notably, breaches of psychological and social privacy undermine moral-based trust, whereas breaches of informational and physical privacy tend to affect performance-based trust [18]. These dimensions were also examined in relation to social robots by Callander et al., who highlighted potential infringements across different privacy types [18].

Below, we discuss how participants' concerns, even when implicit, mapped onto these dimensions.

Physical Privacy. Participants identified several threats of social robots to their physical privacy and safety (See §4.2). Some participants were particularly concerned about the navigation and mapping capabilities of social robots. Given their ability to move autonomously, domestic robots may enter private spaces uninvited and create a pervasive sense of surveillance. Some participants were particularly concerned about social robots accessing children's rooms (See §4.2). To mitigate these risks, participants emphasized the need for mechanisms that allow users to control a social robot's movement (See §4.4). Users should have the ability to lock certain rooms from the robot's access and define boundaries within their living spaces. As Callander et al. propose, cameras on social robots should default to the off mode, reducing concerns related to unintended surveillance [18]. Furthermore, as expressed by participants (See §4.4), we suggest physical indicators, such as camera shutters or status lights, to signal when a device is actively recording audio or video.

Additionally, participants were more accepting of certain data collection practices when they aligned with their expectations (See §4.2). If a social robot were to intrude a user's personal space, for example to measure body temperature using its sensors through touch, transparency and explainability would be essential [18]. We reaffirm calls for increased transparency; social robots should clarify their capabilities, intentions, and purpose in a user-friendly manner before performing any task that might infringe upon a user's physical privacy.

Psychological Privacy. Participants also raised concerns about how social robots 'learn' and retain personal data (See §4.2). With the advancement and proliferation of generative AI, threats to psychological privacy are becoming increasingly relevant. Psychological privacy refers to maintaining control over information relating to our own mental states [121]. Currently, it is already possible to infer a user's mood using only data from their mobile phone sensors [44]. Additionally, users prefer when conversational agents match their emotional tone [13]. This, however, could conflict with users' privacy expectations. One participant, for example, described Google's data inference capabilities as "creepy" and wanted social robots to be transparent around their data inference algorithms (See §4.2). If social robot manufacturers want to include emotional AI features in their devices, it is imperative that they treat the inferred emotion as they would any other data. To align with participant expectations (See §4.4), manufacturers would need to: 1) Clearly indicate when emotional data was being inferred, 2) Allow users to review and delete the emotional data collected on them, and 3) Give users the ability to disable the emotional inference features. Beyond emotion recognition, social robots can lead to psychological dependence, chilling effects, and reduced self-reflection, particularly for vulnerable groups like children [75].

Social Privacy. Social privacy corresponds to the social bonding and boundary management processes between humans and robots [75]. Human–robot interaction studies show that people tend to anthropomorphize robots, attributing human-like qualities to them [15]. This tendency can lead to increased disclosure of personal information, as users develop affection and trust toward the robot [19, 103, 128]. Indeed, our participants identified companionship as one of the main benefits of owning a social robot (See §4.2). They expected these robots to provide companionship not only for themselves but also for children and elderly individuals. Social robots' emotional expressiveness, embodiment, and communication through natural language make them uniquely well-suited to fulfill users' companionship needs. Compared to traditional IoT devices and web-based chatbots–both of which some participants already used for companionship–social robots offer a more dynamic and engaging experience, which may also feel more fulfilling.

At the same time, a notable concern emerged among participants (See §4.2): the potential replacement of genuine human interactions with robot-mediated ones. This concern was particularly pronounced when considering social robots for children. Some participants feared that children might prefer interacting with robots over human peers, leading to over-reliance on robotic companionship and potentially hindering their social development. In psychological therapy settings, participants worried about the loss of human touch, and feared that patients might adhere too strongly to the unreliable advice given by a social robot's language model.

To address participants' concerns on the negative impact of interacting with social robots (See §4.2), designers should implement safeguards that prevent excessive anthropomorphism or at least allow users to control it. Children, in particular, were seen as more vulnerable to the negative effects of interacting with social robots. Therefore, regulatory measures should be established to enforce specific design considerations for social robots marketed toward children. One option would be to design social robots to facilitate interactions *between* children, rather than as a replacement of social interactions, as suggested by Aylett et al. [5].

6 Conclusion

We qualitatively explored the security and privacy needs and concerns of U.S. based participants regarding domestic social robots. Our participants expressed substantial privacy and security concerns, describing a wide range of necessary measures to justify adoption. We offer actionable recommendations for developing social robots that meet the security and privacy needs of users. These include implementing clear and accessible security and privacy controls, enhancing transparency in data handling practices, and ensuring the reliability and accuracy of the robots' functionalities.

References

[1] Eleni Adamopoulou and Lefteris Moussiades. An overview of chatbot technology. In *IFIP international conference on artificial intelligence applications and innovations*, pages 373–383. Springer, 2020.

[2] Arpita Agnihotri and Saurabh Bhattacharya. Chatbots' effectiveness in service recovery. *International Journal of Information Management*, page 102679, 07 2023.

[3] Abdullah Altrad, P Ravindran Pathmanathan, Yazeed Al Moaiad, Yousef Mohamed Endara, Khairi Aseh, Yousef A Baker El-Ebiary, Mazen Mohammed Farea, Nurul Adilah Abdul Latiff, and Syarilla Iryani Ahmad Saany. Amazon in business to customers and overcoming obstacles. In *2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE)*, pages 175–179. IEEE, 2021.

[4] Noah Apthorpe, Pardis Emami-Naeini, Arunesh Mathur, Marshini Chetty, and Nick Feamster. You, me, and iot: How internet-connected consumer devices affect interpersonal relationships. *ACM Transactions on Internet of Things*, 3(4):1–29, 2022.

[5] Matthew Peter Aylett, Randy Gomez, Eleanor Sandry, and Selma Sabanovic. Unsocial robots: How western culture dooms consumer social robots to a society of one. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI EA '23, New York, NY, USA, 2023. Association for Computing Machinery.

[6] Natã M. Barbosa, Zhuohao Zhang, and Yang Wang. 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)*, pages 417–435. USENIX Association, August 2020.

[7] Jenay Beer, Akanksha Prakash, Cory-Ann Smarr, Tiffany Chen, Kelsey Hawkins, Hai Nguyen, Travis Deyle, Charles Kemp, and Wendy Rogers. Older users' acceptance of an assistive robot: Attitudinal changes following brief exposure. *Gerontechnology*, 16(1):21–36, May 2017.

[8] Tony Belpaeme, James Kennedy, Aditi Ramachandran, Brian Scassellati, and Fumihide Tanaka. Social robots for education: A review. *Science Robotics*, 3(21):eaat5954, 2018.

[9] Emily M Bender, Timnit Gebru, Angelina McMillan-Major, and Shmargaret Shmitchell. On the dangers of stochastic parrots: Can language models be too big? In *Proceedings of the 2021 ACM conference on fairness, accountability, and transparency*, pages 610–623, 2021.

[10] James M. Berzuk and James E. Young. Clarifying social robot expectation discrepancy: Developing a framework for understanding how users form expectations of social robots. In *Companion of the 2023 ACM/IEEE International Conference on Human-Robot Interaction*, HRI '23, page 231–233, New York, NY, USA, 2023. Association for Computing Machinery.

[11] Pankaj Bhaskar and Sheikh I Ahamed. Privacy in pervasive computing and open issues. In *The Second International Conference on Availability, Reliability and Security (ARES'07)*, pages 147–154, 2007.

[12] Nanyi Bi and Janet Yi-Ching Huang. I create, therefore i agree: Exploring the effect of ai anthropomorphism on human decision-making. In *Companion Publication of the 2023 Conference on Computer Supported Cooperative Work and Social Computing*, CSCW '23 Companion, page 241–244, New York, NY, USA, 2023. Association for Computing Machinery.

[13] Ghazala Bilquise, Samar Ibrahim, and Khaled Shaalan. Emotionally intelligent chatbots: a systematic literature review. *Human Behavior and Emerging Technologies*, 2022(1):9601630, 2022.

[14] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3:77–101, 01 2006.

[15] Cynthia Breazeal. Toward sociable robots. *Robotics and autonomous systems*, 42(3-4):167–175, 2003.

[16] Cynthia Breazeal. Social robots for health applications. In *2011 Annual international conference of the IEEE engineering in medicine and biology society*, pages 5368–5371. IEEE, 2011.

[17] A.J. Bernheim Brush, Bongshin Lee, Ratul Mahajan, Sharad Agarwal, Stefan Saroiu, and Colin Dixon. Home automation in the wild: challenges and opportunities. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '11, page 2115–2124, New York, NY, USA, 2011. Association for Computing Machinery.

[18] Nicholas Callander, Andrés A Ramírez-Duque, and Mary Ellen Foster. Navigating the human-robot interaction landscape. practical guidelines for privacy-conscious social robots. In *Companion of the 2024 ACM/IEEE International Conference on Human-Robot Interaction*, pages 283–287, 2024.

[19] Ryan Calo. Robots and privacy. In Patrick Lin, Keith Abney, and George A. Bekey, editors, *Robot Ethics: The Ethical and Social Implications of Robotics*, pages 187–202. MIT Press, Cambridge, MA, 2012.

[20] Felix Carros, Johanna Meurer, Diana Löffler, David Unbehaun, Sarah Matthies, Inga Koch, Rainer Wieching, Dave Randall, Marc Hassenzahl, and Volker Wulf. Exploring human-robot interaction with the elderly: Results from a ten-week case study in a care home. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, page 1–12, New York, NY, USA, 2020. Association for Computing Machinery.

[21] George Chalhoub, Martin J Kraemer, Norbert Nthala, and Ivan Flechais. "it did not give me an option to decline": A longitudinal analysis of the user experience of security and privacy in smart home products. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–16, 2021.

[22] Eun Kyoung Choe, Sunny Consolvo, Jaeyeon Jung, Beverly Harrison, Shwetak N. Patel, and Julie A. Kientz. Investigating receptiveness to sensing and inference in the home using sensor proxies. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, UbiComp '12, page 61–70, New York, NY, USA, 2012. Association for Computing Machinery.

[23] Hanbyul Choi, Jonghwa Park, and Yoonhyuk Jung. The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, 81:42–51, 2018.

[24] Richard Chow, Serge Egelman, Raghudeep Kannavara, Hosub Lee, Suyash Misra, and Edward Wang. Hci in business: A collaboration with academia in iot privacy. pages 679–687, 08 2015.

[25] Sawyer Collins, Kenna Baugus Henkel, Zachary Henkel, Casey C Bennett, Cedomir Stanojevic, Jennifer A Piatt, Cindy L Bethel, and Selma Sabanović. " an emotional support animal, without the animal": Design guidelines for a social robot to address symptoms of depression. In *Proceedings of the 2024 ACM/IEEE International Conference on Human-Robot Interaction*, pages 147–156, 2024.

[26] Federal Trade Commission. Ftc announces crackdown on deceptive ai claims and schemes. *FTC Release*, 2024.

[27] Samuel Rhys Cox, Yi-Chieh Lee, and Wei Tsang Ooi. Comparing how a chatbot references user utterances from previous chatting sessions: An investigation of users' privacy concerns and perceptions. In *Proceedings of the 11th International Conference on Human-Agent Interaction*, HAI '23, page 105–114, New York, NY, USA, 2023. Association for Computing Machinery.

[28] Dagoberto Cruz-Sandoval, Arturo Morales-Tellez, Eduardo Benitez Sandoval, and Jesus Favela. A social robot as therapy facilitator in interventions to deal with dementia-related behavioral symptoms. In *Proceedings of the 2020 ACM/IEEE international conference on human-robot interaction*, pages 161–169, 2020.

[29] Anupam Das, Martin Degeling, Daniel Smullen, and Norman Sadeh. Personalized privacy assistants for the internet of things: Providing users with notice and choice. *IEEE Pervasive Computing*, 17(3):35–46, 2018.

[30] Julia Dawe, Craig Sutherland, Alex Barco, and Elizabeth Broadbent. Can social robots help children in healthcare contexts? a scoping review. *BMJ paediatrics open*, 3(1), 2019.

[31] Maartje MA De Graaf and Somaya Ben Allouch. The evaluation of different roles for domestic social robots. In *2015 24th IEEE International Symposium on Robot and Human Interactive Communication (RO-MAN)*, pages 676–681. IEEE, 2015.

[32] Maartje MA de Graaf, Somaya Ben Allouch, and Jan AGM Van Dijk. Why would i use this in my home? a model of domestic social robot acceptance. *Human–Computer Interaction*, 34(2):115–173, 2019.

[33] Nicola Dell, Vidya Vaidyanathan, Indrani Medhi, Edward Cutrell, and William Thies. "yours is better!": participant response bias in hci. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '12, page 1321–1330, New York, NY, USA, 2012. Association for Computing Machinery.

[34] Tamara Denning, Cynthia Matuszek, Karl Koscher, Joshua R Smith, and Tadayoshi Kohno. A spotlight on security and privacy risks with future household robots: attacks and lessons. In *Proceedings of the 11th international conference on Ubiquitous computing*, pages 105–114, 2009.

[35] Dmitry Dereshev, David Kirk, Kohei Matsumura, and Toshiyuki Maeda. Long-term value of social robots through the eyes of expert users. In *Proceedings of the 2019 CHI conference on human factors in computing systems*, pages 1–12, 2019.

[36] Jayati Dev and Sruti Dev. "how can i help you?": User perceptions of privacy in retail chat agents. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI EA '23, New York, NY, USA, 2023. Association for Computing Machinery.

[37] Judith Dörrenbächer, Ronda Ringfort-Felner, and Marc Hassenzahl. The intricacies of social robots: Secondary analysis of fictional documentaries to explore the benefits and challenges of robots in complex social settings. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2023.

[38] Pardis Emami-Naeini, Janarth Dheenadhayalan, Yuvraj Agarwal, and Lorrie Faith Cranor. Are consumers willing to pay for security and privacy of {IoT} devices? In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 1505–1522, 2023.

[39] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. Exploring how privacy and security factor into iot device purchase behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, page 1–12, New York, NY, USA, 2019. Association for Computing Machinery.

[40] Hua Fan, Bing Han, Wei Gao, and Wenqian Li. How ai chatbots have reshaped the frontline interface in china: examining the role of sales–service ambidexterity and the personalization–privacy paradox. *International Journal of Emerging Markets*, ahead-of-print, 01 2022.

[41] Eduard Fosch-Villaronga, Aurelia Tamò-Larrieux, and Christoph Lutz. Did i tell you my new therapist is a robot? ethical, legal, and societal issues of healthcare and therapeutic robots. *Ethical, Legal, and Societal Issues of Healthcare and Therapeutic Robots (October 17, 2018)*, 2018.

[42] Jill J Francis, Marie Johnston, Clare Robertson, Liz Glidewell, Vikki Entwistle, Martin P Eccles, and Jeremy M Grimshaw. What is an adequate sample size? operationalising data saturation for theory-based interview studies. *Psychology and health*, 25(10):1229–1245, 2010.

[43] Yajie Gao, Yaping Chang, Tangwutu Yang, and Zhihao Yu. Consumer acceptance of social robots in domestic settings: A human-robot interaction perspective. *Journal of Retailing and Consumer Services*, 82:104075, 2025.

[44] Asma Ghandeharioun, Daniel McDuff, Mary Czerwinski, and Kael Rowan. Emma: An emotion-aware wellbeing chatbot. In *2019 8th International Conference on Affective Computing and Intelligent Interaction (ACII)*, pages 1–7, 2019.

[45] Miriam Gieselmann and Kai Sassenberg. The more competent, the better? the effects of perceived competencies on disclosure towards conversational artificial intelligence. *Social Science Computer Review*, 41:2342 – 2363, 2022.

[46] Eun Go and S Shyam Sundar. Humanizing chatbots: The effects of visual, identity and conversational cues on humanness perceptions. *Computers in Human Behavior*, 97:304–316, 2019.

[47] Reinhard Grabler and Sabine Theresia Koeszegi. Privacy beyond data: Assessment and mitigation of privacy risks in robotic technology for elderly care. *ACM Transactions on Human-Robot Interaction*, 14(1):1–23, 2025.

[48] Ashley Griffin, Zhaopeng Xing, Sean Mikles, Stacy Bailey, Saif Khairat, Jaime Arguello, Yue Wang, and Arlene Chung. Information needs and perceptions of chatbots for hypertension medication self-management: A mixed methods study. *JAMIA Open*, 4, 04 2021.

[49] Pamela Grimm. Social desirability bias. *Wiley international encyclopedia of marketing*, 2010.

[50] Paige Gross. States strike out on their own on ai, privacy regulation. *Washington State Standard*, 2024.

[51] Ece Gumusel, Kyrie Zhixuan Zhou, and Madelyn Rose Sanfilippo. User privacy harms and risks in conversational ai: A proposed framework, 2024.

[52] Hana Habib, Sarah Pearman, Jiamin Wang, Yixin Zou, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. " it's a scavenger hunt": Usability of websites' opt-out and data deletion choices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–12, 2020.

[53] Hana Habib, Sarah Pearman, Ellie Young, Ishika Saxena, Robert Zhang, and Lorrie FaIth Cranor. Identifying user needs for advertising controls on facebook. *Proceedings of the ACM on Human-Computer Interaction*, 6(CSCW1):1–42, 2022.

[54] Jeonghye Han, Miheon Jo, Sungju Park, and Sungho Kim. The educational use of home robots for children. In *ROMAN 2005. IEEE International Workshop on Robot and Human Interactive Communication, 2005.*, pages 378–383. IEEE, 2005.

[55] Anna Henschel, Guy Laban, and Emily S. Cross. What makes a robot social? a review of social robots from science fiction to a home or hospital near you. *Current Robotics Reports*, 2(1):9–19, 2021.

[56] Christian Pieter Hoffmann, Christoph Lutz, and Giulia Ranzini. Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 10(4), 2016.

[57] Aike C Horstmann and Nicole C Krämer. Great expectations? relation of previous experiences with social robots in real life or in the media and expectancies based on qualitative and quantitative assessment. *Frontiers in psychology*, 10:939, 2019.

[58] Nayab Iqbal, Hassaan Ahmed, and Kaukab Abid Azhar. Exploring teachers' attitudes towards using chatgpt. *Global Journal for Management and Administrative Sciences*, 3(4):97–111, 2022.

[59] Carolin Ischen, Theo Araujo, Hilde Voorveld, Guda van Noort, and Edith Smit. Privacy concerns in chatbot interactions. In *Chatbot Research and Design: Third International Workshop, CONVERSATIONS 2019, Amsterdam, The Netherlands, November 19–20, 2019, Revised Selected Papers 3*, pages 34–48. Springer, 2020.

[60] Sooyeon Jeong, Deirdre E Logan, Matthew S Goodwin, Suzanne Graca, Brianna O'Connell, Honey Goodenough, Laurel Anderson, Nicole Stenquist, Katie Fitzpatrick, Miriam Zisook, et al. A social robot to mitigate stress, anxiety, and pain in hospital pediatric care. In *Proceedings of the tenth annual ACM/IEEE international conference on human-robot interaction extended abstracts*, pages 103–104, 2015.

[61] Takayuki Kanda, Tomohiro Hirano, Donald Eaton, and Hiroshi Ishiguro. Interactive robots as social partners and peer tutors for children: A field trial. *Human-Computer Interaction*, 19(1-2):61–84, 2004.

[62] Elise Karinshak, Sunny Xun Liu, Joon Sung Park, and Jeffrey T Hancock. Working with ai to persuade: Examining a large language model's ability to generate pro-vaccination messages. *Proceedings of the ACM on Human-Computer Interaction*, 7(CSCW1):1–29, 2023.

[63] Samuel C Karpen. The social psychology of biased self-assessment. *American Journal of Pharmaceutical Education*, 82(5):6299, 2018.

[64] Woojin Kim, Yuhosua Ryoo, SoYoung Lee, and Jung Lee. Chatbot advertising as a double-edged sword: The roles of regulatory focus and privacy concerns. *Journal of Advertising*, 52:1–19, 04 2022.

[65] Martin Johannes Krämer. *Empowering privacy in the connected home: communal use of smart technologies*. PhD thesis, University of Oxford, 2022.

[66] Nir Kshetri. Cybercrime and privacy threats of large language models. *IT Professional*, 25(3):9–13, 2023.

[67] Oksana Kulyk, Kristina Milanovic, and Jeremy Pitt. Does my smart device provider care about my privacy? investigating trust factors and user attitudes in iot systems. In *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*, pages 1–12, 2020.

[68] Minae Kwon, Malte F. Jung, and Ross A. Knepper. Human expectations of social robots. In *The Eleventh ACM/IEEE International Conference on Human Robot Interaction*, HRI '16, page 463–464. IEEE Press, 2016.

[69] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. Alexa, are you listening? privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. *Proc. ACM Hum.-Comput. Interact.*, 2(CSCW), nov 2018.

[70] Hee Rin Lee and Laurel D Riek. Reframing assistive robots to promote successful aging. *ACM Transactions on Human-Robot Interaction (THRI)*, 7(1):1–23, 2018.

[71] Hosub Lee and Alfred Kobsa. Privacy preference modeling and prediction in a simulated campuswide iot environment. pages 276–285, 03 2017.

[72] Leigh Levinson, Tyler Barrett, Randy Gomez, and Selma Sabanović. Surveying adult perceptions of privacy and attitudes towards social robots in the home. In *Companion of the 2024 ACM/IEEE International Conference on Human-Robot Interaction*, pages 664–668, 2024.

[73] Leigh Levinson, Jessica McKinney, Christena Nippert-Eng, Randy Gomez, and Selma Šabanović. Our business, not the robot's: family conversations about privacy with social robots in the home. *Frontiers in Robotics and AI*, 11:1331347, 2024.

[74] Alex John London, Yosef S Razin, Jason Borenstein, Motahhare Eslami, Russell Perkins, and Paul Robinette. Ethical issues in near-future socially supportive smart assistants for older adults. *IEEE Transactions on Technology and Society*, 4(4):291–301, 2023.

[75] Christoph Lutz, Maren Schöttler, and Christian Pieter Hoffmann. The privacy implications of social robots: Scoping review and expert interviews. *Mobile Media & Communication*, 7(3):412–434, 2019.

[76] Christoph Lutz and Aurelia Tamò-Larrieux. Do privacy concerns about social robots affect use intentions? evidence from an experimental vignette study. *Frontiers in Robotics and AI*, 8, 2021.

[77] Christoph Lutz and Aurelia Tamó-Larrieux. The robot privacy paradox: Understanding how privacy concerns shape intentions to use social robots. In *Human-Machine Communication*, volume 1, pages 87–111, 2020.

[78] Nishtha Madaan, Mohd Abdul Ahad, and Sunil M Sastry. Data integration in iot ecosystem: Information linkage as a privacy threat. *Computer law & security review*, 34(1):125–133, 2018.

[79] Rob Marjerison, Youran Zhang, and Hanyi Zheng. Ai in e-commerce: Application of the use and gratification model to the acceptance of chatbots. *Sustainability*, 14:14270, 11 2022.

[80] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for cscw and hci practice. *Proc. ACM Hum.-Comput. Interact.*, 3(CSCW), nov 2019.

[81] Kevin R McKee, Xuechunzi Bai, and Susan T Fiske. Humans perceive warmth and competence in artificial intelligence. *Iscience*, 26(8), 2023.

[82] Nidhi Mishra, Teena Bharti, Aviral Kumar Tiwari, and Gregor Pfajfar. Public and scholarly interest in social robots: An investigation through google trends, bibliometric analysis, and systematic literature review. *Technological Forecasting and Social Change*, 206:123578, 2024.

[83] Javier Movellan, Micah Eckhardt, Marjo Virnes, and Angelica Rodriguez. Sociable robot improves toddler vocabulary skills. In *Proceedings of the 4th ACM/IEEE international conference on Human robot interaction*, pages 307–308, 2009.

[84] Wendy Moyle, Marguerite Bramble, Cindy Jones, and Jenny Murfield. Care staff perceptions of a social robot called paro and a look-alike plush toy: a descriptive qualitative approach. *Aging & mental health*, 22(3):330–335, 2018.

[85] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. Privacy expectations and preferences in an IoT world. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 399–412, Santa Clara, CA, July 2017. USENIX Association.

[86] Stanislava Naneva, Marina Sarda Gou, Thomas L Webb, and Tony J Prescott. A systematic review of attitudes, anxiety, acceptance, and trust towards social robots. *International Journal of Social Robotics*, 12(6):1179–1201, 2020.

[87] Magdalene Ng, Kovila P. L. Coopamootoo, Ehsan Toreini, Mhairi Aitken, Karen Elliot, and Aad van Moorsel. Simulating the effects of social presence on trust, privacy concerns & usage intentions in automated bots for finance, 2020.

[88] Hiroyuki Nitto, Daisuke Taniyama, and Hitomi Inagaki. Social acceptance and impact of robots and artificial intelligence. *Nomura Res. Inst. Pap*, 211:1–5, 2017.

[89] Chris Norval and Jatinder Singh. A room with an overview: Towards meaningful transparency for the consumer internet of things. *IEEE Internet of Things Journal*, 2023.

[90] Martin T Orne. Demand characteristics and the concept of quasi-controls. *Artifacts in behavioral research: Robert Rosenthal and Ralph L. Rosnow's classic books*, 110:110–137, 2009.

[91] Samson O Oruma, Mary Sánchez-Gordón, Ricardo Colomo-Palacios, Vasileios Gkioulos, and Joakim K Hansen. A systematic review on social robots in public spaces: Threat landscape and attack surface. *Computers*, 11(12):181, 2022.

[92] Debajyoti Pal, Suree Funilkul, Vajirasak Vanijja, and Borworn Papasratorn. Analyzing the elderly users' adoption of smart-home services. *IEEE access*, 6:51238–51252, 2018.

[93] Hae Won Park, Rinat Rosenberg-Kima, Maor Rosenberg, Goren Gordon, and Cynthia Breazeal. Growing growth mindset with a social robot peer. In *Proceedings of the 2017 ACM/IEEE international conference on human-robot interaction*, pages 137–145, 2017.

[94] Denis Peña and Fumihide Tanaka. Human perception of social robot's emotional states via facial and thermal expressions. *ACM Transactions on Human-Robot Interaction (THRI)*, 9(4):1–19, 2020.

[95] Nazerke Rakhymbayeva, Aida Amirova, and Anara Sandygulova. A long-term engagement with a social robot for autism therapy. *Frontiers in Robotics and AI*, 8:669972, 2021.

[96] Pranav Rane, Varun Mhatre, and Lakshmi Kurup. Study of a home robot: Jibo. *International journal of engineering research and technology*, 3(10):490–493, 2014.

[97] Rowena Rodrigues. Legal and human rights issues of ai: Gaps, challenges and vulnerabilities. *Journal of Responsible Technology*, 4:100005, 10 2020.

[98] Rahime Saglam, Jason Nurse, and Duncan Hodges. *Privacy Concerns in Chatbot Interactions: When to Trust and When to Worry*, pages 391–399. 07 2021.

[99] Shruti Sannon, Brett Stoll, Dominic DiFranzo, Malte F. Jung, and Natalya N. Bazarova. "i just shared your responses": Extending communication privacy management theory to interactions with conversational agents.

Proc. ACM Hum.-Comput. Interact., 4(GROUP), jan 2020.

[100] Benjamin Saunders, Julius Sim, Tom Kingstone, Shula Baker, Jackie Waterfield, Bernadette Bartlam, Heather Burroughs, and Clare Jinks. Saturation in qualitative research: exploring its conceptualization and operationalization. *Quality & quantity*, 52:1893–1907, 2018.

[101] Burkhard Schafer and Lilian Edwards. "i spy, with my little sensor": fair data handling practices for robots between privacy, copyright and security. *Connection Science*, 29(3):200–209, 2017.

[102] Sofia Serholt and Wolmet Barendregt. Robots tutoring children: Longitudinal evaluation of social engagement in child-robot interaction. In *Proceedings of the 9th nordic conference on human-computer interaction*, pages 1–10, 2016.

[103] Amanda JC Sharkey. Should we welcome robot teachers? *Ethics and Information Technology*, 18:283–297, 2016.

[104] Takanori Shibata and Kazuyoshi Wada. Robot therapy: a new approach for mental healthcare of the elderly–a mini-review. *Gerontology*, 57(4):378–386, 2011.

[105] Jatin Pal Singh. Quantifying healthcare consumers' perspectives: An empirical study of the drivers and barriers to adopting generative ai in personalized healthcare. *ResearchBerg Review of Science and Technology*, 2(1):171–193, 2022.

[106] Marita Skjuve, Asbjørn Følstad, and Petter Bae Brandtzaeg. The user experience of chatgpt: Findings from a questionnaire study of early users. In *Proceedings of the 5th International Conference on Conversational User Interfaces*, pages 1–10, 2023.

[107] Michael J Sobrepera, Vera G Lee, Suveer Garg, Rochelle Mendonca, and Michelle J Johnson. Perceived usefulness of a social robot augmented telehealth platform by therapists in the united states. *IEEE robotics and automation letters*, 6(2):2946–2953, 2021.

[108] Daniel J Solove. A taxonomy of privacy. *U. Pa. l. Rev.*, 154:477, 2005.

[109] Sophie Stephenson, Majed Almansoori, Pardis Emami-Naeini, and Rahul Chatterjee. " it's the equivalent of feeling like you're in {Jail"}: Lessons from firsthand and secondhand accounts of {IoT-Enabled} intimate partner abuse. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 105–122, 2023.

[110] Kaiwen Sun, Yixin Zou, Jenny Radesky, Christopher Brooks, and Florian Schaub. Child safety in the smart home: parents' perceptions, needs, and mitigation strategies. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2):1–41, 2021.

[111] Yubing Sun and Qingyu Liang. Research on the relationship between self-ai connection and customer engagement–based on the analysis of customer ai trust and ai anthropomorphism. In *Proceedings of the 2023 6th International Conference on Information Management and Management Science*, IMMS '23, page 48–53, New York, NY, USA, 2023. Association for Computing Machinery.

[112] Tadele Shiferaw Tadele, Theo de Vries, and Stefano Stramigioli. The safety of domestic robotics: A survey of various safety-related publications. *IEEE robotics & automation magazine*, 21(3):134–142, 2014.

[113] Fumihide Tanaka and Shizuko Matsuzoe. Children teach a care-receiving robot to promote their learning: Field experiments in a classroom for vocabulary learning. *Journal of Human-Robot Interaction*, 1(1):78–95, 2012.

[114] Brian Tang, Dakota Sullivan, Bengisu Cagiltay, Varun Chandrasekaran, Kassem Fawaz, and Bilge Mutlu. Confidant: A privacy controller for social robots. In *2022 17th ACM/IEEE International Conference on Human-Robot Interaction (HRI)*, pages 205–214. IEEE, 2022.

[115] Meg Tonkin, Jonathan Vitale, Sarita Herse, Syed Ali Raza, Srinivas Madhisetty, Le Kang, The Duc Vu, Benjamin Johnston, and Mary-Anne Williams. Privacy first: designing responsible and inclusive social robot applications for in the wild studies. In *2019 28th IEEE International Conference on Robot and Human Interactive Communication (RO-MAN)*, pages 1–8. IEEE, 2019.

[116] Andreas Triantafyllidis, Anastasios Alexiadis, Konstantinos Votis, and Dimitrios Tzovaras. Social robot interventions for child healthcare: A systematic review of the literature. *Computer Methods and Programs in Biomedicine Update*, page 100108, 2023.

[117] Onuralp Ulusoy and Pinar Yolum. Panola: A personal assistant for supporting users in preserving privacy. *ACM Transactions on Internet Technology (TOIT)*, 22(1):1–32, 2021.

[118] Gijs van Ewijk, Matthijs Smakman, and Elly A Konijn. Teachers' perspectives on social robots in education: an exploratory case study. In *Proceedings of the interaction design and children conference*, pages 273–280, 2020.

[119] Sarah Theres Völkel, Renate Haeuslschmid, Anna Werner, Heinrich Hussmann, and Andreas Butz. How to trick ai: Users' strategies for protecting themselves from automatic personality assessment. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, page 1–15, New York, NY, USA, 2020. Association for Computing Machinery.

[120] Kazuyoshi Wada and Takanori Shibata. Living with seal robots—its sociopsychological and physiological influences on the elderly at a care house. *IEEE transactions on robotics*, 23(5):972–980, 2007.

[121] Abel Wajnerman Paz. Is mental privacy a component of personal identity? *Frontiers in Human Neuroscience*, 15:773441, 2021.

[122] Wikipedia contributors. Social robot — Wikipedia, the free encyclopedia, 2024. [Online; accessed 30-April-2024].

[123] Sara Wilson. Colorado becomes first state with sweeping artificial intelligence regulations. *Colorado Newsline*, 2024.

[124] Peter Worthy, Ben Matthews, and Stephen Viller. Trust me: Doubts and concerns living with the internet of things. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems*, DIS '16, page 427–434, New York, NY, USA, 2016. Association for Computing Machinery.

[125] Eric Zeng, Shrirang Mare, and Franziska Roesner. End user security and privacy concerns with smart homes. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 65–80, Santa Clara, CA, July 2017. USENIX Association.

[126] Xiao Zhan, Yifan Xu, and Stefan Sarkadi. Deceptive ai ecosystems: The case of chatgpt. *arXiv preprint arXiv:2306.13671*, 2023.

[127] Fengjiao Zhang, Zhao Pan, and Yaobin Lu. Aiot-enabled smart surveillance for personal data digitalization: Contextual personalization-privacy paradox in smart home. *Information & Management*, 60(2):103736, 2023.

[128] Zhiping Zhang, Michelle Jia, Bingsheng Yao, Sauvik Das, Ada Lerner, Dakuo Wang, Tianshi Li, et al. " it's a fair game", or is it? examining how users navigate disclosure risks and benefits when using llm-based conversational agents. *arXiv preprint arXiv:2309.11653*, 2023.

[129] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. User perceptions of smart home iot privacy. *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW), November 2018. Publisher Copyright: © 2018 Copyright held by the owner/author(s). Publication rights licensed to ACM.

[130] Xu Zheng, Zhipeng Cai, and Yingshu Li. Data linkage in smart internet of things systems: a consideration from a privacy perspective. *IEEE Communications Magazine*, 56(9):55–61, 2018.

[131] Xinyu Zhu, Xingguo Zhang, Zinan Chen, Zhanxun Dong, Zhenyu Gu, and Danni Chang. The trusted listener: The influence of anthropomorphic eye design of social robots on user's perception of trustworthiness. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, CHI '22, New York, NY, USA, 2022. Association for Computing Machinery.

A Interview Material

A.1 Interview Consent Form

The interview informed consent form is available at the following link:https://github.com/socialrobotattitudes/SRMaterial/blob/main/Interview%20Consent%20Form.pdf

A.2 Screening Survey

The screening survey is available at the following link:https://github.com/socialrobotattitudes/SRMaterial/blob/main/Screening%20Survey.pdf

A.3 Interview Questions

A.3.1 Knowledge and Awareness Toward Social Robots

1. Have you ever heard of the term social robot?
   (a) (*If yes*) In your own words, how would you define a social robot?
   (b) (*If no*) If you had to guess, how would you define a social robot?
2. What capabilities do you think a device should have to be counted as a social robot?

Providing a definition for a social robot While there is no single definition of what a social robot is, for the purposes of this interview, we'll define a social robot as an artificial intelligence (AI) system that is designed to interact with humans and other robots by following social behaviors and rules attached to its role. Like other robots, a social robot is physically embodied.

1. Is this definition clear to you, or is there any part of this definition that you would like us to further elaborate on?

2. Do you know of any technologies currently available for purchase that fit the provided definition of a social robot?

Robot Specification An established company is aiming to develop a novel social robot. They are currently working on designing the prototype device, and they would like to do some research with users to specify some important aspects of the social robot before they launch the main product to the market. As an independent research institute, we are helping this company to capture people's honest opinions and feedback regarding the prototype device to inform the future design of the company's social robot. Therefore, it is valuable for us to capture any positive and negative feedback that comes to your mind.

We provide the specification of the social robot For the remainder of this interview, we may ask you a few questions to capture your attitudes and preferences toward purchasing this specific social robot, or social robots more generally. For these questions, please assume that the final price of the device is within your budget.

1. Which of these features are you most comfortable with and why?

2. Which of these features are you most concerned about and why?

3. Would you consider purchasing this specific social robot in the near future, and why?

4. What information would you like to have to make an informed decision as to whether or not to have this specific social robot in your home?

A.3.2 Contextual Privacy And Security Attitudes

In this section, we are going to walk through some potential use-case scenarios for the prototype social robot we described earlier. We will ask some follow-up questions after each scenario.

[**Purchasing for yourself**] Imagine that you are living alone, and you are purchasing this specific social robot for yourself to be the robot's primary user.

[**Purchasing for children**] Imagine that you are living in a family setting with a child, and you are purchasing this specific social robot for the child to be the robot's primary user.

[**Purchasing for the elderly**] Imagine that you are living with an elderly family member, and you are purchasing this specific social robot for the elderly family member to be the robot's primary user.

[**Purchasing for a communal household**] Imagine that you are living in a communal setting, and you are purchasing this specific social robot to be shared amongst your household without having a specific primary user.

So far we have talked about purchasing the device for yourself, a child, or an elderly family member. Now we're going to talk about the various contexts that this device could be used in.

[**Educational Context**] Keeping in mind the four user scenarios we just described, how comfortable or concerned would you be purchasing this device to fulfill an educational need for the users?

[**Medical Context**] Keeping in mind the four user scenarios we just described, how comfortable or concerned would you be purchasing this device to fulfill a medical need for the users?

[**Psychological Therapy Context**] Keeping in mind the four user scenarios we just described, how comfortable or concerned would you be purchasing this device to fulfill a psychological therapy need for the users?

1. How comfortable or concerned are you with this described scenario, and why?

   (a) (*If concerned*) What do you think should happen to make you less concerned about this described scenario?

A.3.3 Privacy And Security Expectations Toward Social Robots

1. On a scale of 1 to 5, 1 being not at all important and 5 being very important, how important do you consider privacy and security to be in your decision to purchase a social robot and why?

2. What type of privacy and security information, if any, would you want to know about to determine if you would purchase a social robot?

3. As a reminder, social robots collect information, and use artificial intelligence to enable social interactions. What type of information, if any, would you want to know about the conversational artificial intelligence features of a social robot to determine if you would purchase it?

4. How would you like this information to be communicated to you to inform your purchasing decisions?

5. Who do you think is responsible for protecting users from the potential privacy and security risks of social robots, and how?

Feature	Description
Visual Recognition	The robot can detect and remember different faces and objects in its environment. In addition, it can react and respond to the visual cues.
Voice Recognition	The robot can detect and remember the different voices in its environment. In addition, it can react and respond to voice commands.
Expressive Communication	The robot can communicate via expressions. Such expressions could be communicated through voice or facial expressions.
Personalization	The robot learns to personalize its interactions with its users. It will adapt to your preferences and behaviors.
Navigation and Mapping	The robot can map its environment and navigate through spaces without collision.
Internet Connected	The device is connected to the internet, allowing for app downloads.

Table 2: We designed a specification for the social robot based on the prominent capabilities in existing social robots.

ID	Smart Home Devices	AI-Enabled Chatbots
P1	Activity tracker, Home assistants, Connected printers, Smart doorlock	ChatGPT, Google Bard, Google Gemini
P2	Smart TV, Smart thermostat, Connected lights, Games console, Home assistants, Video streaming product, Smart plugs, Smart doorlock	ChatGPT, Google Bard, Google Gemini, Microsoft Bing AI
P3	Smart TV, Activity tracker, Smart thermostat, Connected lights, Games console, Home assistants, Smartwatch, Video streaming product, Connected printers, Smart plugs, Smart doorlock, Baby camera, Smart kitchen appliances	ChatGPT, Google Bard, Google Gemini, Snapchat My AI
P4	Smart TV, Connected lights, Games console, Home assistants, Smartwatch, Video streaming product, Connected printers, Smart plugs, Smart doorlock	ChatGPT, Google Bard, Google Gemini, Microsoft Bing AI
P5	Home assistants	ChatGPT
P6	Smart TV, Activity tracker, Smart thermostat, Connected lights, Games console, Home assistants, Smartwatch, Video streaming product, Connected printers, Smart plugs, Smart doorlock, Smart water sprinkler, Smart kitchen appliances	ChatGPT
P7	Smart TV, Games console, Home assistants, Smartwatch, Video streaming product, Connected printers	ChatGPT
P8	Smart TV, Connected lights, Home assistants, Video streaming products, Connected printers, Smart plugs, Smart kitchen appliances	ChatGPT, GitHub Copilot, Google Bard, Google Gemini, Microsoft Bing AI
P9	Smart TV, Activity tracker, Connected lights, Games console, Home assistants, Video streaming product, Connected printers, Smart plugs, Smart security camera	ChatGPT, Google Bard, Microsoft Bing AI
P10	Smart TV, Activity tracker, Connected lights, Home assistants, Smart watch, Video streaming product, Connected printers, Smart plugs, Smart security camera, Smart health monitors, Smart kitchen appliances, Smart bluetooth trackers	ChatGPT, Google Bard
P11	Smart TV, Games console, Home assistants, Video streaming product, Connected printers	ChatGPT, Google Bard, Snapchat My AI
P12	Smart TV, Activity tracker, Smart thermostat, Games console, Home assistants, Connected printers, Smart health monitors	ChatGPT, Google Bard, Microsoft Bing AI
P13	Smart TV, Activity tracker, Games console, Home assistants, Video streaming product, Connected printers, Smart security camera, Grocery ordering, Smart kitchen appliances	ChatGPT, Claude, Google Bard, Google Gemini, Jasper, Microsoft Bing AI
P14	Smart TV, Games console, Home assistants, Smartwatch, Video streaming product, Connected printers, Smart water sprinkler	ChatGPT, Claude, Google Bard, Google Gemini
P15	Smart TV, Activity tracker, Smart thermostat, Connected lights, Home assistants, Smartwatch, Connected printers, Smart plugs, Smart doorlock, Smart security camera, Smart smoke monitors	ChatGPT, Google Bard
P16	Home assistants, Video streaming products, Connected printers, Smart doorlock, Smart security camera, Baby camera, Smart kitchen appliances	ChatGPT, Google Bard, Microsoft Bing AI
P17	Smart TV, Activity tracker, Connected lights, Games console, Home assistants, Video streaming product, Connected printers, Smart plugs, Smart security camera, Smart health monitors, Smart kitchen appliances	ChatGPT, Google Bard, Microsoft Bing AI, Snapchat My AI, DeepAI
P18	Smart TV, Connected lights, Games console, Home assistants, Smartwatch, Video streaming product, Connected printers, Smart security camera	ChatGPT, Claude
P19	Activity tracker, Games console, Home assistants, Video streaming product, Connected printers, Smart doorlock, Smart security camera	MetaAI

Table 3: Participants and the smart home devices and AI-enabled chatbots they use.

A.4 Debriefing Statement

The debriefing statement is available at the following link: https://github.com/socialrobotattitudes/SRMaterial/blob/main/Debriefing%20Statement.pdf

B Interview Codebook

The codebook is available at the following link: https://github.com/socialrobotattitudes/SRMaterial/blob/main/Codebook%20(F).pdf