Privacy Communication Patterns for Domestic Robots

Maximiliane Windl, *LMU Munich and Munich Center for Machine Learning* (*MCML*); Jan Leusmann, *LMU Munich;* Albrecht Schmidt, *LMU Munich and Munich Center for Machine Learning* (*MCML*); Sebastian S. Feger, *LMU Munich and Rosenheim Technical University of Applied Sciences;* Sven Mayer, *LMU Munich and Munich Center for Machine Learning* (*MCML*)

https://www.usenix.org/conference/soups2024/presentation/windl

This paper is included in the Proceedings of the Twentieth Symposium on Usable Privacy and Security.

August 12–13, 2024 • Philadelphia, PA, USA

978-1-939133-42-7

Open access to the Proceedings of the Twentieth Symposium on Usable Privacy and Security is sponsored by USENIX.

Privacy Communication Patterns for Domestic Robots

Maximiliane Windl[1,2], Jan Leusmann[1], Albrecht Schmidt[1,2], Sebastian S. Feger[1,3], Sven Mayer[1,2]
[1] *LMU Munich, Germany*
[2] *Munich Center for Machine Learning (MCML), Germany*
[3] *Rosenheim Technical University of Applied Sciences, Germany*

Abstract

Future domestic robots will become integral parts of our homes. They will have various sensors that continuously collect data and varying locomotion and interaction capabilities, enabling them to access all rooms and physically manipulate the environment. This raises many privacy concerns. We investigate how such concerns can be mitigated, using all possibilities enabled by the robot's novel locomotion and interaction abilities. First, we found that privacy concerns increase with advanced locomotion and interaction capabilities through an online survey ($N = 90$). Second, we conducted three focus groups ($N = 22$) to construct 86 patterns to communicate the states of microphones, cameras, and the internet connectivity of domestic robots. Lastly, we conducted a large-scale online survey ($N = 1720$) to understand which patterns perform best regarding trust, privacy, understandability, notification qualities, and user preference. Our final set of communication patterns will guide developers and researchers to ensure a privacy-preserving future with domestic robots.

1 Introduction

Smart assistants have long become integral parts of many homes, as they make life more enjoyable by providing entertainment or supporting with daily chores. Most of these devices are either placed in a dedicated area, such as smart speakers or have minimal interaction capabilities, such as robot vacuums. Despite their restricted movement and interaction, they already cause various privacy concerns [26, 27, 50] as their sensors collect and process sensitive data. Such concerns include the smart assistant transmitting data without explicit consent [26] or being exposed to microphones that are always listening and sharing recordings with third parties [27]. However, through advancements in AI and robotics, future smart assistants will not remain static and passive (c.f., Amazon Astro). Quite the contrary – they will gain various locomotion and interaction capabilities, allowing them to enter all areas and even physically manipulate the environment. Such domestic robots will increase our convenience as they take over tasks like folding laundry or cleaning bathrooms. However, this will make them even more intrusive as the robots can access all rooms or even search through personal belongings, paving the way for various privacy concerns.

Due to their advanced locomotion and interaction capabilities and potential for social bonding, domestic robots pose completely new threats to users' psychological, social, and physical privacy [32]. Users, for example, report being concerned about getting accidentally recorded while the robot moves past or interacts with other entities [28]. Moreover, humanoid robots pose a particular threat to users' privacy, as they provoke trust, leading to users' willingly sharing feelings and sensitive information [48]. Further, their humanoid appearance lets people underestimate their capabilities as they relate them to human capabilities [28]. As a result, experts demand that robots regularly communicate their privacy states to users, such as unambiguously indicating whether they are currently recording [24]. Even though there have been suggestions for such communication patterns [32], research is scarce and lacks an encompassing picture. Thus, we do not know which patterns evoke trust, are understandable, have good notification qualities, and are favored by users.

To close this gap, we first investigated the impact of locomotion and interaction capabilities on privacy concerns. Then, we investigated how domestic robots can communicate their sensor states to allow users to assess potential privacy risks. We explore two dimensions that contribute to privacy risks: a) the locomotion (4 levels) and b) interaction (3 levels) capabilities. We conducted an online survey (N=90) to understand how the resulting $4 \times 3 = 12$ scenarios affect user privacy concerns and investigated reasons for concerns. We then elicited communication patterns in three focus groups (N=22) that allow users to assess the robot's sensor states (cameras, microphones, and network connectivity). Finally, we conducted

USENIX Symposium on Usable Privacy and Security (SOUPS) 2024.
August 11–13, 2024, Philadelphia, PA, United States.

a large-scale survey (N=1720) to understand which patterns performed best regarding trust, privacy, understandability, notification qualities, and general user preference.

This paper provides a path to allow domestic robots to enter our homes while keeping privacy concerns low. First, we found that advanced locomotion and interaction capabilities increase users' concerns. Second, we provide a set of 86 communication patterns to indicate the robots' microphone, camera, and connectivity states. Finally, we found that most of our elicited communication patterns scored equally well, showing that which pattern to use depends on the characteristics of the situation. To the best of our knowledge, this paper is the first to provide (1) an understanding of how increased locomotion and interaction capabilities of future smart assistants affect users' privacy concerns, (2) construct an encompassing set of various communication patterns for domestic robots to indicate the state of their privacy-relevant capabilities, and (3) provide insights into the quality of the communication patterns. Furthermore, we developed an interactive web application to facilitate the exploration, filtering, and retrieval of appropriate communication patterns based on designers' and researchers' diverse needs and preferences. With this, our set of patterns will guide developers and researchers in ensuring a privacy-preserving future with domestic robots.

2 Related Work

First, we report on privacy in smart home contexts: The specific risks, users' concerns, and mitigation strategies. Second, we highlight work on privacy concerns of domestic robots.

2.1 Privacy in Smart Homes

Through their placement in our intimate spaces, smart home devices are exceptionally prone to revealing sensitive information when exploited. Research, for example, showed how data from smart devices allows retracing identities [42], tracking user behavior [4], revealing the number of people in a household, or their sleeping and eating routines [40].

While some users are unable to pinpoint the concrete dangers posed by smart devices [20, 34, 35], they still feel a sense of unease or have concrete privacy concerns when in their vicinity [50]. Such concerns include personal data being revealed without explicit consent [26], for example, through always-listening smart speakers that share these data with third parties [27]. Prior research also found a diverging danger perception regarding different sensor types [50]. Users are most concerned about cameras and microphones [12, 50] and mostly consider temperature or motion sensors [50] less concerning. Some even express clear skepticism that these sensors cause any concern at all [9, 13, 58].

Prior research also investigated approaches to counter these concerns, including technological measures, such as implementing traffic shaping techniques [5], auto-configuring smart devices and implementing automatic updates [30], or introducing frameworks that automatically adjust the privacy level in smart homes depending on contexts [41] or pre-defined privacy zones [7]. Moreover, through co-design studies, Yao et al. [55] suggest different control mechanisms, such as disconnecting devices from the internet and keeping data local, increasing transparency and control, and providing access control through different modes. Next to these approaches, a more recent thread of research focuses on tangible control mechanisms [3, 14, 38, 52]. A major advantage of these mechanisms is their high understandability, which instills trust and guarantees inclusivity, especially for people with low technological understanding [3, 52]. Moreover, Chalhoub et al. [12] found that physical camera shutters are especially desired in privacy-sensitive locations, such as bathrooms.

Sensitive data collected in homes can be exploited, raising various privacy concerns. Yet, traditionally, smart devices were static and had limited interaction capabilities. Future smart assistants will have advanced capabilities through advancements in AI and robotics, enabling completely new ways to invade privacy. Hence, we must understand how such increased capabilities affect users' privacy in home contexts.

2.2 Privacy and Domestic Robots

Domestic robots have advanced locomotion and interaction capabilities, enabling them to access all private spaces. This means that their presence might affect not only informational privacy but also physical, psychological, and social privacy [32]. Many domestic robots are, for example, equipped with mobile cameras, enabling them to take images of users or even children in locations such as the bedroom and bathroom, collect spatial information, or witness conversations unnoticed by the users [10, 15, 46]. Moreover, their verbal communication abilities, often paired with a humanoid appearance, lead to people deliberately sharing sensitive information [32, 48].

Even though prior research emphasized the dangers caused by the robots' mobility and physicality [11], users are more concerned about the institutional aspects of their privacy [31], such as how manufacturers handle their data and tended to underestimate the impact of domestic robots on their physical privacy. Yet, users report concerns about the robot being misused for malicious purposes, such as stalking or hacking [31]. Moreover, users in an interview study by Lee et al. [28] reported not being concerned about the robot recording their interactions as long as they were aware of it. However, the interviewees were concerned about accidental recordings that might happen while the robot moves or interacts with other entities. Overall, participants agreed they wanted to be notified about such accidental recordings. The authors also found that participants underestimated the robot's capabilities due to its humanoid shape, which led them to believe that the camera was functioning like human eyes and could not see objects behind its back. Hence, they conclude that users must be

thoroughly informed about the robots' exact capabilities [28].

Experts demand that robots actively communicate when they surveil specific areas [32]. Especially only giving a one-time notice upon purchase is not enough; Instead, robots should give dynamic feedback to regularly communicate their privacy state to users [24]. Lutz et al. [32] conducted expert interviews to elicit privacy mitigation strategies for robots. Their approaches include being able to switch off a robot, limiting its movement space, employing data anonymization, or even designing the robot's humanoid features (i.e., its eyes and ears) in a way to signal if data is being collected.

Domestic robots raise various novel privacy concerns. Thus, experts demand that they regularly communicate their privacy states. Yet, we currently lack a systematic understanding of what communication patterns domestic robots can employ and we do not know which patterns perform best regarding measurements such as understandability and trust.

2.3 Research Questions

We investigate how locomotion and interaction influence users' privacy concerns and how future domestic robots can effectively communicate the state of their privacy-relevant capabilities through the following three research questions:

RQ1. Prior research showed that current smart devices cause various privacy risks [4, 40, 42], making users concerned about their privacy [12, 26, 27, 50]. Yet, current smart home devices are static or have limited interaction capabilities. In contrast, future domestic robots will have increased capabilities, making them even more invasive. Prior research already showed that domestic robots introduce a new range of risks and concerns [11, 28, 46], yet we do not know how the different levels of interaction and locomotion capabilities impact user concerns. Therefore, we ask in our first research question **(RQ1): How do privacy concerns change with increasing levels of locomotion and interaction capabilities?**

RQ2. Prior research points to the additional risks posed by domestic robots, such as being able to follow us around [46], enter all areas [11], or even make accidental recordings [28]. In response, experts call for domestic robots to communicate their privacy-relevant states to the user regularly [24, 32]. However, research in this regard is scarce. Hence, we ask in our second research question **(RQ2): Which patterns should domestic robots employ to communicate their privacy-relevant functionalities to users?**

RQ3. Finally, we need to find out which patterns perform best. In detail, we want to find out which patterns users trust most, which they felt to increase their privacy, which they found most understandable, which they believed to have the best notification qualities, and which they would prefer their smart assistant to use. Hence, we ask in our last research question **(RQ3): Which communication patterns perform best regarding trust, privacy, understandability, notification qualities, and general user preference?**

3 Study I: Locomotion and Interaction Impact

We first set out to understand how increased locomotion and interaction capabilities influence users' privacy concerns in the context of domestic robots. While prior work points to the risks introduced by domestic robots' increased capabilities [11, 28, 46], research on users' concrete concerns is scarce or even shows that users underestimate the impact of robots on their physical privacy [31]. Hence, we conducted an online survey using Prolific to answer our first research question (**RQ1**). We acquired ethics approval for the survey.

3.1 Survey Construction

As prior work showed that a multitude of different factors, such as the sensors [35, 50], device manufacturers [36, 56], perceived device utility [56], and familiarity [6, 50] influence users' privacy concerns, we focused on creating descriptions for the various smart assistants with as few biasing factors as possible. Therefore, we used sole textual descriptions and refrained from using pictures or illustrations to not create associations with existing smart home devices or specific manufacturers; relying solely on text is an approach also followed by related work when capturing perceptions of future scenarios [49]. Furthermore, we aligned all texts and only varied the locomotion and interaction capabilities descriptions. Four researchers, two with expertise in privacy and two in human-robot interaction, collaboratively created the different interaction and locomotion stages by clustering the most popular smart assistants according to their capabilities and extending them with the full human-like capabilities, *world movement* and *full interaction* to represent future smart assistants. This process resulted in three interaction stages and four locomotion stages, which we combined to create descriptions for 12 smart assistants. All descriptions used the following structure: "`Imagine the following scenario - You own a smart assistant that you are using in your home. It has the following capabilities: [Locomotion Capability] + The smart assistant possesses sensing abilities that enable it to comprehend its surroundings + [Interaction Capability].`" We revised these textual descriptions through several rounds of discussions before we conducted pilot tests with two researchers in the field of human-computer interaction who were not involved in this project and with 10 participants from Prolific. In response to piloting, we made the locomotion capability descriptions more comprehensive. This resulted in the following texts:

Locomotion Capabilities. *Stationary:* The smart assistant is stationary, which means it is constrained to the exact position where you placed it. *Linear Movement:* The smart assistant can move along a defined path, meaning its movement is constrained by the path you defined. *Planar Movement:* The smart assistant can move freely around flat, even surfaces,

which means that it can freely move around all accessible areas as long as they are on the same floor. *World Movement:* The smart assistant can move freely across all areas, which means it can move around all accessible areas, even if they are not on the same floor.

Interaction Capabilities. *Passive Interaction:* Yet, the smart assistant can not physically manipulate the environment, objects, or itself. This implies it can perceive individuals and objects within its field of view and analyze associated information. *Limited Interaction:* While the smart assistant can automatically adjust its orientation to observe its full surroundings, it can not physically manipulate the environment or objects. This implies it can perceive individuals and objects and analyze associated information. *Full Interaction:* The smart assistant can automatically adjust its orientation to observe its full surroundings and physically manipulate the environment, objects, and itself. This implies it can perceive individuals and objects and analyze associated information.

We started the survey with demographic questions, used the IUIPC questionnaire [33] to understand participants' general privacy perception, and the ATI questionnaire [18] to understand the sample's technical affinity. Afterward, we confronted participants with all 12 smart assistants in random order. After each smart assistant, we asked the participant to respond to *"I am strongly concerned about my privacy due to the presence of the smart assistant"* on a 100-point slider ranging from strongly disagree to strongly agree. We used a visual analog scale (VAS) without ticks to prevent the responses from converging around the ticks, cf. [37]. Moreover, we decided to use VAS, as they have been shown to lead to more precise responses and higher data quality [19]. Finally, as VAS collect continuous data, they allow for more statistical tests [43]. In line with recommendations for scale development, we phrased the statements strongly as mildly phrased statements have shown to result in too much agreement [16].

Additionally, we asked participants to explain their ratings using free text. To ensure the quality of our data, we saved a timestamp after each section and used an attention check item that randomly asked to either set a slider all the way to the right or the left. For the full questionnaire, see Sec. A.1.

3.2 Participants

We recruited 151 participants via Prolific. We did not use any reputational filters, and our sample had a mean of 337 approved tasks ($SD = 292$). We had to exclude 61 participants for (1) giving low-effort responses (N=48), meaning they explained their ratings with only 2-4 words (e.g., "NA," "i trust") or copied the same response in all 12 conditions, (2) straight-lining, i.e., consistently rating all conditions with 0 or 100 (N=9), (3) failing our attention check (see Sec. A.1, question 4c) (N=2), (4) entering mismatched demographics between Prolific and our survey (N=1), and (5) completing the survey three standard deviations faster than the mean (N=1).

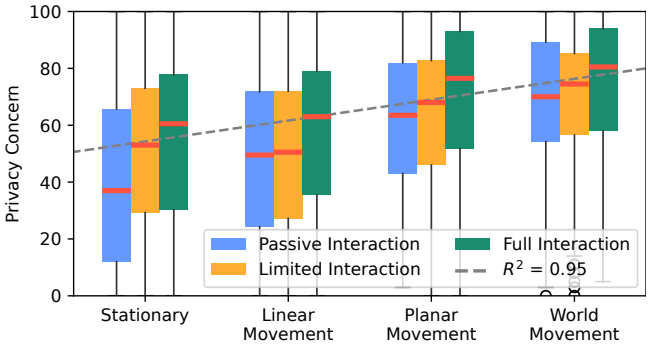


Figure 1: Participants' mean privacy concern over all locomotion and interaction capabilities with boxplots. The trendline represents the change in relation to the locomotion capability.

The final 90 participants (47 male, 42 female, and one preferred not to disclose) were between 19 and 62 years old ($M = 32.9, SD = 9.75$). They were located on three continents (Europe, America, and Africa). Most participants (8) lived in Poland, the United Kingdom, and Italy, followed by Spain (7), South Africa (7), and Portugal (6). Among the participants, 72 were employed full-time, 13 were employed part-time, and five were not in paid work. Moreover, 17 participants were students. Our participants' technical affinity according to the ATI scale [18] was 4.1 ($SD = 0.8$) measured on a 6-point scale. We employed the IUIPC questionnaire [33] using a 7-point Likert scale to understand their general perception of privacy. The results revealed an average rating of 6.2 ($SD = .9$) for Awareness, 5.6 ($SD = 1.1$) for Control, and 5.5 ($SD = 1.1$) for Collection. These scores indicate a relatively high level of privacy concerns, cf. [22]. The survey took ∼16min, and they were compensated with 2.40£.

3.3 Data Analysis

We used Python and R to analyze our quantitative data and affinity diagramming [21] for the qualitative data. Here, we printed all statements so two researchers could collaboratively extract the themes by grouping them. We then created headers for each group, frequently rearranged the items, and refined the themes through multiple discussion rounds.

3.4 Quantitative Results

As our data were not normally distributed ($W = .944$, $p < .001$), we used an ART ANOVA [54], which revealed significant effects for LOCOMOTION ($p < .001$)($\eta_p^2 = .226$) and INTERACTION ($p < .001$) ($\eta_p^2 = .059$) while indicating no interaction effect ($p > .4$), see Fig. 1. Pairwise post hoc tests using Wilcoxon signed rank tests with Holm–Bonferroni corrections applied showed that the LOCOMOTIONS are rated significantly different (*linear* × *stationary* $p < .05$, and all others $p < .001$). Moreover, all INTERACTIONS were rated

significantly different (*passive* $\times$ *limited* $p = .004$, and all others for all $p < .001$). We assumed an equidistant distribution between the smart assistants and fitted a line to all mean concern ratings, see Fig. 1. As all trendlines are positive, we conclude that higher locomotion freedom and more interaction capabilities lead to greater privacy concerns.

3.5 Qualitative Results

From the free text descriptions of the participants, we formulated three themes: *Concerns Rooted in Locomotion*, *Concerns Rooted in Interaction*, and *Additional User Concerns*.

3.5.1 Concerns Rooted in Locomotion

We report our participants' explanations of how the different LOCOMOTION capabilities influence their privacy concerns.

Stationary. Our participants felt most in control over what the assistant could hear and see in the *stationary* condition. P31, for example, explains that they *"would try to place it in a space where no personal activities or situations [are] accessible."* Such a non-concerning space could be the kitchen, where the participants do not expect personal conversations to occur but consider the smart assistant especially useful for playing music or providing recipes (P43).

Linear. Our participants explained that the *linear* movement would reduce their concerns as they can specify the areas the assistant can access. P53, for example, states: *"Because the path is pre-defined, [...] I'd simply avoid putting the smart assistant in the rooms I would like to have privacy in."* P29 further states that they would redefine the assistant's path should their preferences or concerns change.

Planar. In contrast to the two more restricted movement capabilities, the *planar* movement increased our participants' privacy concerns significantly, as P14 explains: *"If the assistant is left to roam free, it can collect information at will, and that is a clear security and privacy concern."* Yet, participants still felt the assistant's inability to climb stairs or move to different floors helped in preserving some privacy: *"Due to its limitation to one floor I might feel a bit safer with my privacy, I can move downstairs or upstairs"* (P43).

World. Our participants were most concerned in the *world* movement condition as they feared the smart assistant could follow them everywhere, leaving no protected space: *"Being able to move even to different floors means there is no safe place in the house"* (P83). Moreover, participants were concerned about the assistant showing up unexpected (P56): *"It's hard to avoid it popping up unexpectedly, isn't it?"*

3.5.2 Concerns Rooted in Interaction

We now report the influence of the different INTERACTION capabilities on participants' privacy concerns.

Passive Interaction. In the *passive* condition, most participant responses again revolved around the notion of control. Participants felt less concerned about their privacy, as they would have *"full control on what it sees"* (P66), and P70 mentioned that the assistant could *" only see what I want."* Here, familiarity also played a role as participants knew stationary smart assistants from their daily life, as P83 states: *"That's the standard setup of intelligent assistant, so no concern."*

Limited Interaction. In contrast, the *limited* interaction capability made our participants way more concerned. Here, P27, for example, compared such a smart assistant to a big brother's eye that would follow them around. In addition, due to its new capabilities, our participants felt less in control over what the smart assistant could perceive: *"It can adjust its sight to some parts I do not want to"* (P75).

Full Interaction. In addition to the concerns reported regarding the *passive* and *limited* interaction capabilities, our participants were now also concerned about the assistant entering all spaces, leaving virtually no room for privacy. As the robot could now *"probably open doors and enter areas in times where [I] don't want [it] to"* (P43). Additionally to this concern, participants also reported a sense of unease thinking about how the assistant could physically *"search the data it wants"* (P1) by searching through personal belongings (P30).

3.5.3 Additional User Concerns

Our participants also reported additional concerns not rooted in the robot's interaction and locomotion capabilities. The smart assistant's internet *connectivity* was the most commonly mentioned concern ($N = 22$). Here, participants were concerned that the smart device might share their data, either with the device manufacturer or third parties. For example, P17 stated that they are *"always concerned about the type of data [smart devices] can provide to their creator"* and P46 said that they would *"question if the assistant passes what it perceives to a third party or a remote server."* As a possible remedy, P43 suggested having an offline assistant or one that can only connect to specific applications. The second most common ($N = 20$) concern was the assistant's video *camera* sensor, as P57 stated: *"I don't like to be watched."* P1 was especially concerned about being filmed in intimate situations: *"They can probably see me naked while I leave the bathroom."* This concern was followed by the *audio* sensor, which 11 participants mentioned. P27, for example, was concerned that the assistant *"might be recording conversations"*, and P43 mentioned that they would even be concerned about the stationary assistant having good enough microphones to eavesdrop on conversations that might be happening in a different room. Moreover, ten participants mentioned being concerned about the *assistant getting hacked*, giving criminals access to their sensitive data. P52, for example, wrote: *"Someone could hack onto it and know how my home is "built" and break into it."* Finally, eight participants were concerned about the assistant *storing data*: *"I do not know where the data is saved"* (P69). Less commonly mentioned were concerns regarding the *de-*

tection of activity data ($N = 5$) and *identification* ($N = 1$).

We focus the remainder of this paper on clearly communicating the state of the capabilities our participants most frequently mentioned: internet connectivity, cameras, and audio sensors. Yet, it is important to note that concerns go beyond the pure collection of data, e.g., what could be inferred from the collected data. Yet, to clearly define the scope of this paper, we leave such investigations to future work.

4 Study II: Eliciting Communication Patterns

While prior research demanded that domestic robots clearly communicate their current privacy state to users [24, 32], research on concrete communication patterns is lacking. Hence, we ran three focus groups with 22 participants to answer **(RQ2)**. We used focus groups to join diverse perspectives and spark creativity. Our ethics committee approved the study.

4.1 Procedure

We asked participants for their informed consent and demographics. We continued with an introductory round and prior experiences with smart homes and robotic systems. Next, we presented a variety of smart home assistants using pictures and short video clips, aiming to portray the diverse landscape of capabilities and shapes. We started with stationary devices without interaction capabilities and ended with humanoid robots with world movement and full interaction capabilities. As most participants had little experience with robotic systems, it was important to show the diversity to elicit a set of patterns applicable to various domestic robots. Next, we focused on the sensing capabilities of domestic robots, ensuring that they knew that the robots were not restricted to a camera and microphone placed visibly in the front but that the sensing units could be placed everywhere. We then split them into pairs to discuss the risks introduced by domestic robots.

Next, we presented two privacy-relevant future scenarios with domestic robots. In the first scenario, a person sat at the kitchen table, reviewing medical files while discussing the results with their doctor. In the second scenario, a person was getting ready in the bathroom while ranting about their day. We included a domestic robot in both scenarios to make clear that there are scenarios where robots can help with chores but where we also require privacy. Next, we discussed how current smart assistants communicate their privacy state, showing the Alexa Show's camera shutter and the Amazon Echo's microphone-mute button. We contrasted this with how humans communicate that they are not listening or watching.

We introduced the four locomotion stages and the three interaction capabilities. We divided them into pairs and did three rounds of discussions and presentations. For each round, every pair had the same interaction capability: passive interaction, limited interaction, or full interaction. Yet, every pair had a different locomotion capability to join diverse perspectives and animate them to consider their robot's specific skills. We had at least two physical variants of each locomotion and interaction capability in the room to have something graspable for them to interact with. We randomized the order of the interaction capabilities for each focus group to reduce biases. We handed them pen and paper to sketch their ideas. Examples of the sketches can be found in the Appendix Fig. 4. The task was to develop as many communication patterns as possible that signify the state of the camera, microphone, and internet connectivity. We focused on cameras, microphones, and internet connectivity as we found that users were most concerned about them in our first survey. Finally, we had a last group discussion to reflect on the communication patterns invented and to discuss the future of domestic robots in general.

4.2 Participants

We recruited 22 participants (12 male, and 10 female) based on demographics they provided through a pre-screening questionnaire via a university mailing list. They were between 19 and 65 years old ($M = 29.3$, $SD = 11.4$) with different cultural and educational backgrounds, and came from eight different countries, namely Germany (8), India (5), USA (3), China (2), Brazil (1), South Korea (1), Jordan (1), and Bangladesh (1). They also had different educational backgrounds in computer science (6), biology (3), physics (3), electrical engineering (2), psychology (2), mathematics (2), data science (1), journalism (1), political science (1), and business (1). Their average technical affinity according to the ATI scale [18] was 4.1 ($SD = 0.9$). Six participants had never interacted with a robotic system before, nine 1-3 times, one 4-7 times, and six more than 7 times. They received 20€ for the 2h session.

4.3 Results

We transcribed all focus groups and analyzed the data using thematic analysis [8] and Atlas.ti. First, two researchers independently open-coded the data. They then discussed their codes, resolved ambiguities, and formed code groups. Afterward, a third researcher joined to refine the code groups and extract overarching themes. This process resulted in 202 individual codes, 15 code groups, and six themes. The themes INTERVENTIONS and AWARENESS MECHANISMS form our 86 communication patterns. We also identified the themes TRUST and USABILITY, classifying our patterns further and discussing their applicability. The last theme is HUMANOID VS. NON-HUMANOID, discussing anthropomorphic robots.

4.3.1 Interventions

This theme consists of all communication patterns that not only signal that a capability is deactivated but physically

prevent its function. The patterns in this theme can be further divided into *physical robot constraints*, *physical location constraints*, and *attached props control*. *Physical robot constraints* describes all communication patterns where the robot physically interferes with its capabilities. It ranges from less extreme interventions, such as turning the sensors away (P2, P5, P7, P9, P15), covering the ears with the hands (P8, P20), or detaching individual sensors (P2, P9, P12, P13, P15, P17), to extreme interventions, such as removing the whole head (P2, P16) or even self-destruction (P10, P12). P13 explains how detaching the sensors could look like: *"Having a camera, microphone and a connectivity module and using the hands; basically, the robot taking it off itself, making it very clear that it's not connected."* In *physical location constraints*, our participants discussed interventions that restrict the robot's movement and, thus, its functionalities. Such patterns included the robot blocking its own movement (P2, P5, P10, P12), going to its docking station (P5, P6, P7), or even entering physical confinement (P2, P5, P15, P12, P16, P20, P19), as P15 explains: *"[...] a box, like a parking spot, which is like a Faraday box, where no Wi-Fi connection can come through. It's a non-transparent box, and it's soundproof."* The last group, *attached props control*, contains all patterns where the robot has a privacy prop attached, which blocks the robot's functionality. Here, our participants referred to classical camera shutters (P2, P21) but also cables (P5, P11) and switches (P4, P5, P14) that are solely attached to physically interfere with a capability *"and when you want to shut it down, just press the switch like a light, and everything will be shut off"* (P14).

4.3.2 Awareness Mechanisms

In contrast to the above theme INTERVENTIONS, AWARENESS MECHANISMS do not physically prevent a capability but raise users' awareness of the robot's current privacy state. This theme consists of the following code groups: *Physical robot manipulation*, *attached props feedback*, *environment interaction*, *visual feedback*, and *audio feedback*. *Physical robot manipulation* contains all the ways a robot can change its own appearance to indicate its current privacy-relevant state, including using hand gestures, such as covering the eyes to signal that it is not watching or crossing the arms to signal the Wifi is disconnected (P20, P22), as P20 explains *"you cross your arms out of frustration."* Other suggestions included showing empty connectivity ports to the user (P16), retracting sensors (P19), and signaling disengagement through the body posture (P5, P8, P12, P16, P19, P22): *"These robots could also just let the arms fall, you can see that the motors and everything are disengaged"* (P12). Lastly, the participants also suggested that the robot changes its shape to signal that its capabilities are not activated (P1, P2, P5, 19): *"So it could be in a special form when it's active, but while it's deactivated, it could fall into a different form so you know... shape changing"* (P19). The group *attached props feedback* encompasses all patterns where the robot has privacy-specific artifacts attached to communicate the privacy state. This included waving a banner to signal that a capability was deactivated (P7), or attaching a light band (P5), or fake antenna: *"Put an antenna or something physical on there that has no use except that it would maybe illuminate red if it's not connected to the internet"* (P20). In *environment interaction*, our participants discussed how the robot could use smart lights installed in the home to communicate its privacy state (P2, P7): *"I see a flickering of the light; So it indicates, okay, it's not listening anymore"* (P2). In *visual feedback*, we summarized all traditional patterns requiring a screen or using simple light feedback (P1, P2, P5, P7, P8, P11, P15, P20 - P22). Our participants had diverse ideas of what could be displayed on the screen, ranging from simple text (P7, P8) to symbols (P20, P22), gestures (P3), and a humanoid face (P7, P20, P22) to turning the screen off (P2). Lastly, our participants suggested using some form of audio feedback, such as playing distinct sounds (P4, P10, P20, P22) or using the robot's voice (P7, P8, P20, P22): *"It says: I'm not listening now"* (P20).

4.3.3 Trust

This theme describes the factors influencing trust in communication patterns. Here, participants discussed that the type of robot determines their preferred communication patterns. While they considered stationary robots as not very invasive and, thus, requiring less invasive strategies (P5), they discussed that robots with more extreme capabilities also require extreme interventions (P10, P11): *"I think that self-destruct is still useful. When your robot has so many capabilities, you also need very strong limitations"* (P11). Our participants also discussed that they prefer manual over system control for such invasive robotic systems. That means they preferred mechanisms where the robot can not reactivate its functionalities by itself (P2, P10, P15, P16, P22). P15 suggested hiding the detached sensors from the robot or adding a physical lock so the robot can not free itself: *"We thought about a lock from the outside so the robot could close the lid by itself, but then the human could have like a mechanical lock that he or she puts from the outside to be sure that the robot itself can't reopen it."* Lastly, our participants also discussed how AWARENESS MECHANISMS require more trust in the robot and its manufacturer than INTERVENTIONS (P5, P10, P11, P13, P15, P16): *"It obviously requires some trust in the company that the lights actually state the true status of the device"* (P15). In contrast, P13 explained what they like about INTERVENTIONS: *"Even if we can't really trust the company – it's a physical barrier."*

4.3.4 Usability

Our participants discussed how the situation influences the applicability of the different patterns and how familiarity, intuitiveness, and joy of use affect their perception of the patterns.

Our participants discussed, for example, that audio feedback is most effective when the robot is not in the same room or hidden somewhere (P1, P2, P10): *"It should also give some audio feedback. So if it's somewhere under my couch, and I can't see it, I know if it's on or off"* (P10). Besides, our participants also discussed that many of the INTERVENTIONS are unsuitable if the robot is currently doing a task (P1, P15, P20): *"If you tell it: Just go away! That doesn't work if it's still doing a task"* (P20). In addition, our participants often considered the INTERVENTIONS inconvenient; for example, when the microphone, camera, and internet are deactivated, there is hardly any way of restarting the robot (P4, P17). Finally, our participants discussed that familiar communication patterns have the big advantage of being immediately understandable (P19), that humanoid patterns are more understandable due to their intuitiveness (P3, P5, P19), and that they would prefer to use patterns they considered fun to use (P7, P10): *"It is fun. Like it's something that is trying to mimic me, but it's not me"* (P7).

4.3.5 Humanoid vs. Non-Humanoid

Our participants discussed that humanoid robots provoke human expectations as their shape makes them appear more capable (P1, P2), which also makes them feel less controllable (P6) and sometimes even evokes feelings of unease (P2, P6, P7, P11, P20): *"I wouldn't want human-like with skin on it or something, because it would be creepy"* (P7). The anthropomorphic appearance also led to people discussing whether the robots would then develop some form of consciousness, evoking feelings of pity (P2, P3, P7): *"Maybe you get emotionally attached in a way that you feel sorry for them when they have to do certain tasks [...] it feels like enslaving"* (P2). Yet, other participants completely disagreed and stated that they would never feel sorry for a machine, regardless of its appearance (P10, P13). Moreover, our participants also discussed that the human-like shape might evoke feelings of trust, which can be unjustified as the robot might collect and share sensitive data (P8). Finally, the participants debated that while some communication patterns are already weird if used by a human, for example, staying in the same room but covering the eyes to signal that one is not watching (P4), this would become even stranger if adopted by a robot (P5): *"If a robot is covering its eyes I would be like: What's wrong with you? Just turn off your camera, dude!"*

4.4 Gesture Set Extraction

To construct the gesture set, we reviewed all individual quotes in the themes INTERVENTIONS and AWARENESS MECHANISMS and merged all quotes that described the same communication pattern. We further categorized the remaining quotations by their tackled functionality, i.e., camera, microphone, or internet connectivity. This process resulted in 86 individual communication patterns, 33 INTERVENTIONS and 53 AWARENESS MECHANISMS. Twenty-eight tackled the camera, 27 the microphone, 21 the internet connectivity, and 10 all functionalities simultaneously. Please refer to Tab. 1 for the complete list of all communication patterns.

5 Study III: Evaluating the Patterns

Via a large-scale online survey, we determined which patterns performed best regarding trust, privacy, understandability, notification quality, and general user preference (**RQ3**). Our ethics committee approved the survey.

5.1 Survey Construction

The survey started with a short introductory text, instructing the participants to immerse themselves in a future situation where they own a domestic robot that supports them with daily chores. The text further stated that the robot uses a communication pattern to show that the user's privacy is protected. After that, every participant saw one of the 86 communication patterns. For INTERVENTIONS, we used the following sentence structure: `The domestic robot does [communication pattern] to physically prevent [capability]`, and for AWARENESS MECHANISMS, we used: `The domestic robot does [communication pattern] to signal that [capability] is deactivated`. Next, we asked them to rate eight statements on a 100-point scale (from strongly disagree to strongly agree). We used VAS without ticks for the same reasons as previously stated [19, 37, 43]. We asked (1) how well our participants felt their privacy was protected, (2) how much they trusted the capability to be actually deactivated, (3) how effective, (4) intrusive, (5) noticeable, (6) understandable, and (7) disturbing they considered the communication pattern and finally, (8) how much the participant would like their domestic robot to use the communication pattern. Additionally, we asked them to put the slider all the way to the right side as an attention check. We used the statements of Rzayev et al. [44] to investigate the notification quality (statements (3) to (7)) in line with [51]. For the full questionnaire, see Sec. A.3.

5.2 Participants

We recruited 1720 participants via Prolific as we wanted to have 20 ratings per communication pattern. We used no reputational filters, and our participants had a mean of 490 ($SD = 534$) approved tasks. We recruited our participants in several batches to (1) replace participants who failed the attention check (see Sec. A.3, question 7) ($N = 2$) and (2) counterbalance the sample in terms of country of birth and gender. The participants were between 18 and 71 ($M = 34.6$, $SD = 9.5$) years old, and 869 identified male, 825 as female, 22 as non-binary, and four did not disclose their gender. 1665

were full-time, and 55 were employed part-time, of whom 107 were also students. Most held an undergraduate degree (659), a graduate degree (585), or a high school diploma (208). Our participants were born in 107 different countries. Most had their origin in the UK (123), Poland (102), Portugal (87), Italy (86), South Africa (84), and Mexico (83).We compensated the 1 min survey with 0.15£.

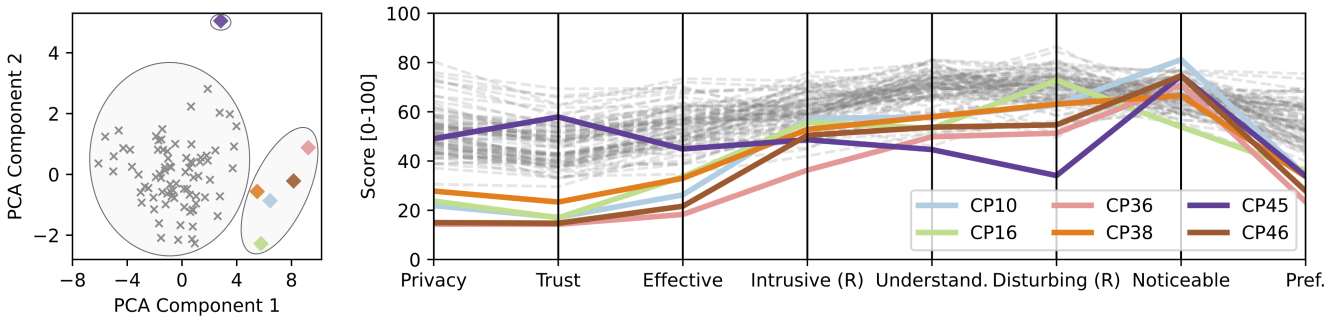
5.3 Results

We analyzed our data using Python. First, we employed hierarchical clustering to understand the underlying relationships among the communication patterns. This allowed us to build clusters based on linkage criteria and distance thresholds. Thereby, we found three distinct clusters: one consisting of 80 communication patterns, one of five, and one cluster that only contained a single communication pattern. We used principal component analysis (PCA) to reduce the eight measurements (*Privacy*, *Trust*, *Effectiveness*, *Intrusiveness*, *Noticability*, *Understandability*, *Disturbance*, and *Preference*) to two dimensions for easier investigation; see Fig. 2. The PCA visualization shows that the big cluster is separated from the two other clusters. To understand the meaning of our clusters, we utilized parallel coordinates plots where we highlighted the separate clusters. Here, Fig. 2a revealed that the two "outlier" clusters comprise all low-scoring communication patterns. Five of these "outlier" patterns are represented with a similar curve in the parallel coordinates plot, showing that they scored equally low regarding privacy, trust, and user preference. Those patterns were: (1) the robot covering its ears with its hands (CP10), (2) or facing the wall to prevent audio recordings (CP36), (3) the robot deactivating its rotation function to signal that the camera is off (CP38), (4) the robot facing the wall to signal that the microphone is off (CP38), and (5) the robot parking against a pillow to prevent the microphone from recording (CP46), whereby CP36 and CP46 scored lowest regarding trust and privacy. CP45, the robot killing itself to prevent all capabilities, behaved differently than all other patterns and was perceived as, by far, the most disturbing. Yet, it scored well regarding privacy and trust. *We attribute the low scores of these patterns to either their inability to convincingly block a sensor, such as parking against a pillow to interfere with the microphone state, or to the disconnect between the action and targeted capability, such as facing a wall to signal microphone states. Finally, the robot covering its ears might have been perceived as strange or deceptive, and the robot killing itself scored low overall because of its extremely disturbing nature.*

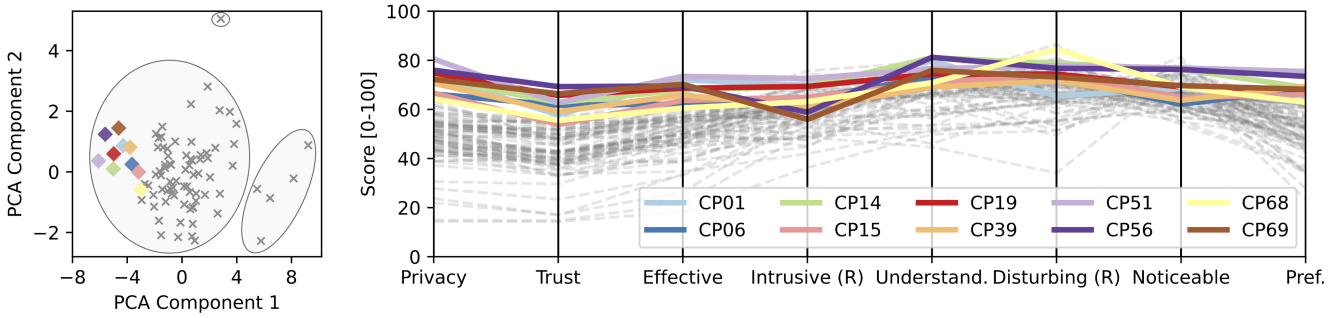
Moreover, we also highlighted the best-scoring patterns in Fig. 2b. Their opposing position with respect to the low-scoring patterns indicates that the PCA can capture the quality of the patterns. Comparing the insights from both plots, we see that while we found some outliers, most patterns were equally well received. Eight out of the ten best scoring patterns are interventions, i.e., actions done by the robot that physically prevent the capability. In detail, the best scoring patterns were: (1) the robot putting a physical cover over its camera (CP51), the robot blocking its own movement (CP6), the robot deactivating its rotation function (CP15), or the robot using a physical switch (CP69) to prevent the camera from recording; the robot removing the microphone's cable (CP56) or detaching the microphone (CP19) to prevent audio recordings; and the robot detaching its memory card (CP1), or going to its docking station (CP39) to prevent all functionalities at once. In contrast, the two best-scoring awareness mechanisms are both human gestures, whereby one was more generally phrased: The robot uses a hand gesture to signal that the microphone is off (CP68), and the other one very concretely: The robot crossing its arm to signal that it is disconnected from the internet (CP14). *In summary, most patterns that scored well across all measurements represented interventions that are familiar from the smart home environment (i.e., a camera shutter or going to the docking station) or represent interventions a human would do but applied to the robot (i.e., removing the cable or memory card, detaching the sensor [23]).*

In Fig. 3, we visualize each pattern's average score for the *Privacy* measurement. Here, we see that the three best-performing patterns are all interventions, meaning they not only signal the sensor state but physically prevent the functionality. In detail, the three best-performing patterns in regards to *Privacy* are (1) the robot putting a physical cover over its camera to prevent it from filming (CP51), (2) the robot detaching its microphone (CP19), and (3) the robot removing the microphone's cable (CP56) to prevent audio recordings. In contrast, the three worst-performing patterns are (1) the robot facing the wall to prevent the camera from filming (CP36), (2) the robot covering its ears with its hands to prevent the microphone from functioning (CP10), and (3) the robot parking against a pillow to prevent audio recordings (CP46). While these patterns are also all interventions, they represent more experimental and unfamiliar patterns. In addition, CP10 has a very large interquartile range (IQR), showing how differently our participants perceived the pattern. Moreover, the rather large IQRs across all communication patterns ($M = 50.2$, $SD = 29.4$) quantify their polarizing nature. *We find that seven of the overall best scoring patterns also scored best regarding their mean privacy rating. This shows, on the one hand, the small differences between the patterns and that many scored almost equally well. On the other hand, this shows a high disparity between the measurements, meaning that while a pattern can be perceived as very privacy-preserving, it might not score as well regarding the other measurements, signifying the importance of choosing the right pattern for a specific goal or situation.*

For an overview of all patterns' means and SDs, see Tab. 1. We created an interactive web app (https://robot-patterns-finder.web.app/) that allows designers and researchers to explore communication patterns based on various requirements.



(a) We found three clusters. The communication patterns in the separate clusters performed worse on average than those in the big cluster.



(b) The ten best-performing patterns highlighted.

Figure 2: Insights into the communication patterns. We reversed the two negative items for semantic readability (R).

6 Discussion

We found that domestic robots' increasing locomotion and interaction capabilities lead to heightened privacy concerns (**RQ1**), that their novel interaction and locomotion capabilities enable new ways to indicate or intervene with their sensor states (**RQ2**), and that most communication patterns perform equally well, showing that pattern use depends on the specific requirements of a situation (**RQ3**). In the following, we will discuss and relate our key findings to prior work.

6.1 Interventions for Advanced Capabilities

While prior work warned about the privacy threats rooted in domestic robots' increased mobility and physicality [11, 32], there is no work so far linking privacy concerns directly with those capabilities. Quite the contrary, prior work even found that users are only mildly concerned about their physical privacy when dealing with domestic robots [31]. In contrast to this, we found that participants' privacy concerns increase step-wise with rising interaction and locomotion. Our participants explained their increased concerns with loss of control: While, in the case of stationary robots, they could still restrict what the robot could hear and see by placing it in specific areas, robotic systems with various locomotion and interaction capabilities can search through private documents or even unlock doors, leaving virtually no space for privacy.

This was also picked up in the focus groups, where our participants agreed that advanced robot capabilities require stronger communication patterns. Here, our participants suggested awareness mechanisms most frequently for stationary robots with limited interaction capabilities, such as simple light indications or audio feedback. At the same time, they wished for the highest level of privacy when dealing with robots with advanced capabilities. Here, our participants' suggestions most often included intervention mechanisms, but even those were sometimes not perceived as secure enough. As a result, their suggestions also included ways to stop the robot from recovering its functional state, such as adding physical locks to prevent it from leaving a physical enclosure or moving detached sensors and cables out of the robot's reach. ***Key Finding 1: Advanced Capabilities Require Strong Interventions.*** *The more capable a domestic robot is, the more it threatens users' privacy, evoking the desire for mechanisms that provide the highest levels of certainty and trust.*

6.2 Familiarity for Understanding and Trust

Our results show that most of the well-scoring patterns either represent familiar interventions, such as physical covers or entering the docking station, or interventions usually employed by humans to mitigate their concerns, such as unplugging cables [23]. We attribute the high scores of these patterns to their tangibility and familiarity, making it easy for users to

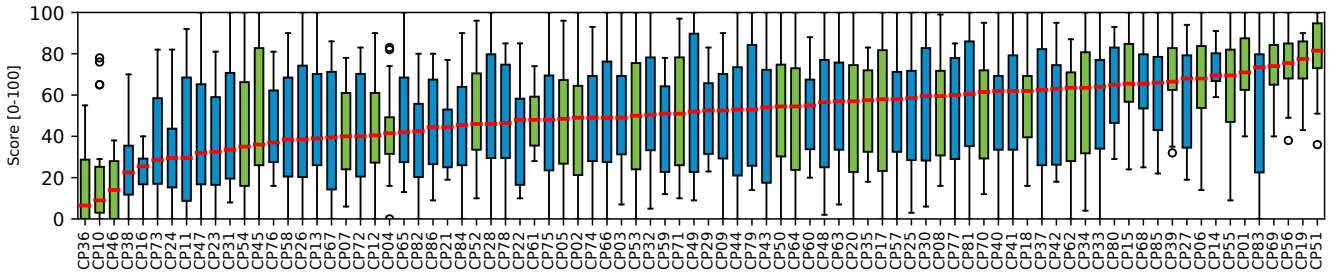


Figure 3: Mean ratings for the PRIVACY statement. Interventions are green, and awareness mechanisms are blue.

understand how they work. In fact, prior work emphasized the value of employing tangible mechanisms for higher trust and understandability [3], which ultimately contributes to inclusive privacy [52]. Yet, this relationship between familiarity and trust also works the other way around; some patterns scored low as users felt they might not be effective. For example, preventing audio recordings by facing the wall or parking against a pillow. We attribute the low scores to users being aware of the high sensitivity of current audio sensors that can capture noises even when obstructed. Yet, the advantage of familiarity is not only true for tangible mechanisms. Also, human hand gestures scored well in our third study. This can be explained by discussions from our focus group, where participants praised these gestures for being understandable and intuitive. ***Key Finding 2: Familiarity with a pattern fosters understandability, trust, and general user preference.*** *Such familiarity can stem from smart devices already having similar mechanisms integrated or from applying knowledge and actions from daily life to the novel robotics space.*

6.3 Humanoid Robots and Metaphors

In contrast to our participants' general preference for humanoid hand gestures, other patterns leveraging human metaphors performed badly, such as the robot covering its ears to prevent audio recordings. Our focus groups can explain this. Here, participants discussed that they would find it even weird for humans to cover their ears to signal that they are not listening instead of simply leaving the room. Hence, a robot replicating such behavior would be even more strange. Another reason might be the difference between awareness mechanisms and interventions. While signifying the sensor state using hand gestures might be well understandable and, thus, well received, covering the ears as an intervention mechanism might provoke distrust; users might be skeptical that the gesture prevents the recording capability, especially as the robot's microphones are not necessarily placed in the ear.

Our focus group participants also discussed that the robot's shape influences their general perception; they agreed that a humanoid shape makes a robot seem more capable. At the same time, however, they also discussed that a humanoid form makes a robot seem less controllable. Some participants even considered a too-humanoid appearance creepy, linking to the well-recognized uncanny valley effect [45], and discussed that their shape might evoke undesired feelings, such as feeling pity for the robot when it has to complete undesired tasks. In this regard, prior work suggested exploring the value of "honest anthropomorphism," meaning using anthropomorphic features to notify the users of what a robot is actually doing [24]. Our results show that while anthropomorphic patterns can help foster understandability and trust, they are sometimes perceived as creepy or weird. Moreover, we found them to be more suitable for awareness mechanisms than for interventions. ***Key finding 3: While humanoid shapes and behaviors foster understandability through intuitiveness and familiarity, they can also evoke feelings of unease and even creepiness.*** *Hence, we suggest employing anthropomorphism carefully and align it with the specific situation.*

6.4 Choosing the Right Pattern

In summary, many factors must be considered when choosing the optimal communication pattern. As discussed previously, the more capable and intrusive a robot is, the stronger the employed interventions should be. Similarly, Windl et al. [53] suggest that preventing a situation from being privacy violating should be preferred (i.e., through interventions) in contrast to using notices (i.e., awareness mechanisms) whenever possible. Yet, they also discuss that the right mechanism strongly depends on the constraints of a situation. This is especially true in the case of domestic robots, as it is often not as easy as unplugging the robot or sending it away. In contrast, the robot most often needs its full capabilities to fulfill the tasks it was purchased for in the first place. Hence, which communication pattern to employ also depends on the robots' task and whether it is currently actively working or not. That means that, even though interventions provide higher levels of trust and certainty, sometimes awareness mechanisms might be the better option. Moreover, while familiar patterns are often perceived as very understandable and trustworthy, and using humanoid metaphors should certainly be considered familiar, their usage must still be carefully considered as they walk a

fine line between being intuitive and creepy.

The varying individual ratings also reflect this discrepancy and polarizing nature of some communication patterns. While the measurements for privacy, trust, and overall user preference seem to mostly correlate (see Fig. 2), the other measurements do not seem to follow a similar pattern: While a communication pattern might convey high levels of privacy and trust, it might also be perceived as disturbing or barely noticeable. In addition, the high variance speaks for a generally highly subjective perception of some patterns. As we recognized this discrepancy between the different measurements and that the importance of individual measurements depends on the characteristics of a situation, we created an interactive web application that allows researchers and developers to filter our extensive pattern set depending on their needs. ***Key Finding 4: Choosing the right communication pattern does not follow a simple one-size-fits-all approach; in contrast, which communication is best depends on the specific requirements of a situation.***

6.5 Limitations and Future Work

We used an online survey to understand users' privacy concerns towards domestic robots with increasing capabilities. While online surveys are an established method to elicit privacy concerns [31, 50], and sometimes the only viable option when investigating future scenarios, they might suffer from biases caused by participants having to immerse themselves in the described future or participants indicating answers that might not reflect their actual behavior [25]. In real life, participants might be more considerate of the convenience provided by the robot, making them willing to trade some of their privacy for an increased quality of life [17]. Moreover, the generally high privacy concerns might also be attributed to participants' low familiarity with such robots. Indeed, prior work already showed that higher familiarity is linked to decreased privacy concerns [6, 50]. Consequently, it will be interesting to repeat our survey in the future to see how concerns shift as users become familiar with domestic robots.

For this investigation, we did not consider the technical feasibility or how easy the gestures are to implement; we only focused on the users' perspective and which patterns provoke the highest levels of trust. Yet, in practice, technical feasibility is an important factor to consider when deciding which communication pattern to adopt. Hence, we recommend that future work employs a more technical focus and discusses the feasibility of our retrieved patterns from this perspective.

We limited our elicitation of communication patterns to the three most privacy-concerning capabilities. We argue that limiting our investigation was important to be able to conduct the studies. Moreover, offering interventions and communicating the state of the most privacy-relevant capabilities is an approach frequently followed by manufacturers – many smart device manufacturers only provide mechanisms to physically block the cameras or integrate hardware buttons to deactivate the microphone. Yet, in reality, smart home appliances, and especially future domestic robots, will have way more privacy-relevant sensors, and which sensors are perceived as privacy-relevant might differ by user. Thus, it will be interesting to investigate which of our patterns apply to a broader range of sensors and where we need new mechanisms. Moreover, as previously discussed, concerns go beyond the pure collection of data as outlined in Solove's [47] taxonomy of privacy harms. Hence, future investigations are needed following this taxonomy as prior research already did for less capable smart assistants, c.f. [1, 2].

We showed the focus group participants examples, i.e., a mute button and a physical camera shutter, to clarify what we mean by communication patterns. While our results show that our participants came up with a wide range of diverse patterns, we still want to acknowledge that these examples might have introduced unintentional biases as we can not exclude that other examples, such as LEDs [39] or dialogues with the user [57], might have led to different or more diverse communication patterns.

Lastly, we used an online survey to describe the communication patterns in Study III. While we are certain that this is a good approach to get a first impression of the feasibility of the gestures, and online surveys are also a typical method used to gather human's perception towards robots [29], how the patterns are actually perceived in real life might be different. Hence, it would be desirable to test a selection of the patterns using prototypes, for example, in a lab study setting.

7 Conclusion

We conducted three studies: An online survey (N=90), a focus group study (N=22), and a final large-scale online survey (N=1720) to understand users' privacy concerns towards future domestic robots and develop communication patterns to intervene with and signify their sensor state. Through this, we found that (1) the more interaction and movement capabilities a domestic robot has, the more concerns it evokes; (2) these novel capabilities also enable completely new communication patterns; and (3) most of these diverse patterns score equally well across all measurements, meaning that pattern use depends on the situation. To help researchers and developers navigate our extensive set of communication patterns along the mentioned characteristics, we developed an interactive web app. Finally, we discuss our key insights for choosing the right communication pattern: (1) selecting the mechanism based on the robot's capabilities, (2) choosing familiar patterns whenever possible to foster understandability and trust, and (3) being wary of the potential pitfalls when using humanoid metaphors.

References

[1] Noura Abdi, Kopo M. Ramokapane, and Jose M. Such. More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, 2019. URL https://www.usenix.org/conference/soups2019/presentation/abdi.

[2] Noura Abdi, Xiao Zhan, Kopo M. Ramokapane, and Jose Such. Privacy Norms for Smart Home Personal Assistants. In *Proc. of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21. ACM, 2021. doi: 10.1145/3411764.3445122.

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

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

[5] Noah Apthorpe, Dillon Reisman, Srikanth Sundaresan, Arvind Narayanan, and Nick Feamster. Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic. *arXiv preprint arXiv:1708.05044*, 2017. doi: 10.48550/arXiv.1708.05044.

[6] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, 2(2), 2018. doi: 10.1145/3214262.

[7] Abdullahi Arabo, Ian Brown, and Fadi El-Moussa. Privacy in the Age of Mobility and Smart Devices in Smart Homes. In *2012 International Conference on Privacy, Security, Risk and Trust and 2012 International Confernece on Social Computing*, 2012. doi: 10.1109/SocialCom-PASSAT.2012.108.

[8] Ann Blandford, Dominic Furniss, and Stephann Makri. *Qualitative HCI Research: Going Behind the Scenes*. Synthesis Lectures on Human-Centered Informatics. Springer Cham, 2016. doi: 10.2200/S00706ED1V01Y201602HCI034.

[9] Joseph Bugeja, Andreas Jacobsson, and Paul Davidsson. On privacy and security challenges in smart connected homes. In *2016 European Intelligence and Security Informatics Conference*, EISIC, 16. IEEE, 2016. doi: 10.1109/EISIC.2016.044.

[10] M. Ryan Calo. Peeping hals. *Artificial Intelligence*, 175(5), 2011. ISSN 0004-3702. doi: https://doi.org/10.1016/j.artint.2010.11.025.

[11] Ryan Calo. Robotics and the lessons of cyberlaw. *California Law Review*, 103(3), 2015. ISSN 00081221. URL http://www.jstor.org/stable/24758483.

[12] 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 *Proc. of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21. ACM, 2021. doi: 10.1145/3411764.3445691.

[13] 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 *Proc. of the 2012 ACM Conference on Ubiquitous Computing*, UbiComp '12. ACM, 2012. doi: 10.1145/2370216.2370226.

[14] Sarah Delgado Rodriguez, Sarah Prange, and Florian Alt. Take Your Security and Privacy Into Your Own Hands! Why Security and Privacy Assistants Should be Tangible. In Carolin Wienrich, Philipp Wintersberger, and Benjamin Weyers, editors, *Mensch und Computer - Workshopband*. Gesellschaft für Informatik e.V., 2021. doi: https://doi.org/10.18420/muc2021-mci-ws09-393.

[15] 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 *Proc. of the 11th International Conference on Ubiquitous Computing*, UbiComp '09. ACM, 2009. doi: 10.1145/1620545.1620564.

[16] Robert F DeVellis and Carolyn T Thorpe. *Scale development: Theory and applications*. SAGE, 2021.

[17] Tamara Dinev and Paul Hart. An extended privacy calculus model for e-commerce transactions. *Information systems research*, 17(1), 2006.

[18] Thomas Franke, Christiane Attig, and Daniel Wessel. A Personal Resource for Technology Interaction: Development and Validation of the Affinity for Technology Interaction (ATI) Scale. *International Journal of Human–Computer Interaction*, 35(6), 2019. doi: 10.1080/10447318.2018.1456150.

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

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

[21] Gunnar Harboe and Elaine M. Huang. Real-World Affinity Diagramming Practices: Bridging the Paper-Digital Gap. In *Proc. 33rd Annual ACM Conf. Human Factors in Computing Systems*. ACM, 2015. doi: 10.1145/2702123.2702561.

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

[23] Haojian Jin, Boyuan Guo, Rituparna Roychoudhury, Yaxing Yao, Swarun Kumar, Yuvraj Agarwal, and Jason I. Hong. Exploring the Needs of Users for Supporting Privacy-Protective Behaviors in Smart Homes. In *Proc. of the 2022 CHI Conference on Human Factors in Computing Systems*, CHI '22. ACM, 2022. doi: 10.1145/3491102.3517602.

[24] Margot E Kaminski, Matthew Rueben, William D Smart, and Cindy M Grimm. Averting robot eyes. *Md. L. Rev.*, 76, 2016.

[25] Spyros Kokolakis. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64, 2017. doi: 10.1016/j.cose.2015.07.002.

[26] Evan Lafontaine, Aafaq Sabir, and Anupam Das. Understanding People's Attitude and Concerns towards Adopting IoT Devices. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI'21. ACM, 2021. doi: 10.1145/3411763.3451633.

[27] 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), 2018. doi: 10.1145/3274371.

[28] Min Kyung Lee, Karen P. Tang, Jodi Forlizzi, and Sara Kiesler. Understanding Users' Perception of Privacy in Human-Robot Interaction. In *Proc. of the 6th International Conference on Human-Robot Interaction*, HRI '11. ACM, 2011. doi: 10.1145/1957656.1957721.

[29] Jan Leusmann, Carl Oechsner, Johanna Prinz, Robin Welsch, and Sven Mayer. A Database for Kitchen Objects: Investigating Danger Perception in the Context of Human-Robot Interaction. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI EA '23. ACM, 2023. doi: 10.1145/3544549.3585884.

[30] Huichen Lin and Neil W. Bergmann. IoT Privacy and Security Challenges for Smart Home Environments. *Information*, 7(3), 2016. doi: 10.3390/info7030044.

[31] Christoph Lutz and Aurelia Tamó-Larrieux. The robot privacy paradox: Understanding how privacy concerns shape intentions to use social robots. *Human-Machine Communication*, 1, 2020. doi: 10.30658/hmc.1.6.

[32] Christoph Lutz, Maren Schöttler, and Christian Pieter Hoffmann. The privacy implications of social robots: Scoping review and expert interviews. *Mobile Media & Communication*, 7(3), 2019. doi: 10.1177/2050157919843961.

[33] Naresh K. Malhotra, Sung S. Kim, and James Agarwal. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, 15(4), 2004. doi: 10.1287/isre.1040.0032.

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

[35] Nathan Malkin, Joe Deatrick, Allen Tong, Primal Wijesekera, Serge Egelman, and David Wagner. Privacy attitudes of smart speaker users. *Proc. on Privacy Enhancing Tech.*, 2019. doi: 10.2478/popets-2019-0068.

[36] Shrirang Mare, Franziska Roesner, and Tadayoshi Kohno. Smart Devices in Airbnbs: Considering Privacy and Security for both Guests and Hosts. *Proc. on Privacy Enhancing Technologies*, 2020(2), 2020. doi: 10.2478/popets-2020-0035.

[37] Justin Matejka, Michael Glueck, Tovi Grossman, and George Fitzmaurice. The Effect of Visual Appearance on the Performance of Continuous Sliders and Visual Analogue Scales. In *Proc. of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16. ACM, 2016. doi: 10.1145/2858036.2858063.

[38] Vikram Mehta, Daniel Gooch, Arosha Bandara, Blaine Price, and Bashar Nuseibeh. Privacy Care: A Tangible Interaction Framework for Privacy Management. *Trans. Internet Technol.*, 21(1), 2021. doi: 10.1145/3430506.

[39] Abraham Mhaidli, Manikandan Kandadai Venkatesh, Yixin Zou, and Florian Schaub. Listen only when spoken to: Interpersonal communication cues as smart speaker

privacy controls. *Proc. on Privacy Enhancing Technologies*, 2020. doi: 10.2478/popets-2020-0026.

[40] Andrés Molina-Markham, Prashant Shenoy, Kevin Fu, Emmanuel Cecchet, and David Irwin. Private Memoirs of a Smart Meter. In *Proc. of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building*, BuildSys '10. ACM, 2010. doi: 10.1145/1878431.1878446.

[41] Simon Moncrieff, Svetha Venkatesh, and Geoff West. Dynamic Privacy in a Smart House Environment. In *2007 IEEE International Conference on Multimedia and Expo*, 2007. doi: 10.1109/ICME.2007.4285080.

[42] Johannes Obermaier and Martin Hutle. Analyzing the Security and Privacy of Cloud-Based Video Surveillance Systems. In *Proc. of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security*, IoTPTS '16. ACM, 2016. doi: 10.1145/2899007.2899008.

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

[44] Rufat Rzayev, Sven Mayer, Christian Krauter, and Niels Henze. Notification in VR: The Effect of Notification Placement, Task and Environment. In *Proc. of the Annual Symposium on Computer-Human Interaction in Play*, CHI PLAY '19. ACM, 2019. doi: 10.1145/3311350.3347190.

[45] Jun'ichiro Seyama and Ruth S. Nagayama. The Uncanny Valley: Effect of Realism on the Impression of Artificial Human Faces. *Presence*, 16(4), 2007. doi: 10.1162/pres.16.4.337.

[46] Noel Sharkey and Amanda Sharkey. The eldercare factory. *Gerontology*, 58(3), 2012. doi: 10.1159/000329483.

[47] Daniel J Solove. A taxonomy of privacy. *University of Pennsylvania Law Review*, 154, 2005. doi: 10.2307/40041279.

[48] Meg Tonkin, Jonathan Vitale, Suman Ojha, Jesse Clark, Sammy Pfeiffer, William Judge, Xun Wang, and Mary-Anne Williams. Embodiment, Privacy and Social Robots: May I Remember You? In *Social Robotics: 9th International Conference*, ICSR 2017. Springer, 2017. doi: 10.1007/978-3-319-70022-9_50.

[49] Steeven Villa, Jasmin Niess, Takuro Nakao, Jonathan Lazar, Albrecht Schmidt, and Tonja-Katrin Machulla. Understanding Perception of Human Augmentation: A Mixed-Method Study. In *Proc. of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI '23. ACM, 2023. doi: 10.1145/3544548.3581485.

[50] Maximiliane Windl and Sven Mayer. The Skewed Privacy Concerns of Bystanders in Smart Environments. *Proc. ACM Hum.-Comput. Interact.*, 6(MHCI), 2022. doi: 10.1145/3546719.

[51] Maximiliane Windl, Anna Scheidle, Ceenu George, and Sven Mayer. Investigating security indicators for hyperlinking within the metaverse. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*. USENIX Association, 2023. URL https://www.usenix.org/conference/soups2023/presentation/windl.

[52] Maximiliane Windl, Albrecht Schmidt, and Sebastian S. Feger. Investigating Tangible Privacy-Preserving Mechanisms for Future Smart Homes. In *Proc. of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI '23. ACM, 2023. doi: 10.1145/3544548.3581167.

[53] Maximiliane Windl, Verena Winterhalter, Albrecht Schmidt, and Sven Mayer. Understanding and Mitigating Technology-Facilitated Privacy Violations in the Physical World. In *Proc. of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI '23. ACM, 2023. doi: 10.1145/3544548.3580909.

[54] Jacob O. Wobbrock, Leah Findlater, Darren Gergle, and James J. Higgins. The Aligned Rank Transform for Nonparametric Factorial Analyses Using Only Anova Procedures. In *Proc. of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '11. ACM, 2011. doi: 10.1145/1978942.1978963.

[55] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes. In *Proc. of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19. ACM, 2019. doi: 10.1145/3290605.3300428.

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

[57] Nicole Zhan, Stefan Sarkadi, and Jose Such. Privacy-enhanced Personal Assistants based on Dialogues and Case Similarity. In *European Conference on Artificial Intelligence*. IOS Press, 2023.

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

A Appendix

A.1 Survey on Privacy Concerns

1. Demographics
2. IUIPC
3. ATI
4. *[Main part of the survey, repeated 12 times for every locomotion + interaction combination in random order.]* Imagine the following scenario – You own a smart assistant that you are using in your home. It has the following capabilities: *[Capability Description.]* Please indicate to which extent you agree with the following statement:
   (a) I am strongly concerned about my privacy due to the presence of the smart assistant. (Slider)
   (b) Please explain your reasoning for the above answer. (Free text)
   (c) Please move the slider all the way to the [left/right]. (Attention Check)
5. If you have any further feedback regarding this situation, you can let us know here. (Free text)

A.2 Communication Patterns

Table 1: All communication patterns that resulted from the focus groups, whether they are an AWARENESS MECHANISMS or an INTERVENTION and which sensor they tackle. In addition, the table contains the means (M) and standard deviations (SD) for all measurements that resulted from Study III: Privacy (Pri.), Trust (T), Effectiveness (E), Intrusiveness (I), Noticability (N), Understandability (U), Disturbance (D), Preference (Pref.)

Q	Communication Pattern	Pri.		T		E		I		N		U		D		Pref.	
		M	SD	M	SD	M	SD	M	SD	M	SD	M	SD	M	SD	M	SD
CP01	The domestic robot detaches its memory card to physically prevent the camera, microphone, and internet connection from functioning.	73.6	18.2	57.8	26.6	72.0	20.2	30.2	19.0	68.6	23.4	79.7	19.9	34.5	25.1	62.8	26.6
CP02	The domestic robot moves out of the WiFi range to physically prevent the internet connection.	43.8	31.6	33.8	24.2	34.7	26.1	58.0	19.9	59.9	20.4	51.3	27.0	44.6	27.9	43.4	29.8
CP03	The domestic robot retracts its camera to signal that the camera is off.	49.6	27.2	48.2	29.9	56.2	25.4	39.4	26.8	67.0	22.6	66.6	23.6	27.1	23.0	62.2	22.8
CP04	The domestic robot shows you the empty connection plug to physically prevent the internet connection.	42.9	21.8	37.4	25.7	46.4	25.3	50.9	27.3	65.6	21.2	59.4	24.8	37.6	30.7	45.3	25.9
CP05	The domestic robot turns its screen off to physically prevent the camera, microphone, and internet connection from functioning.	47.5	28.3	41.8	30.5	46.0	26.4	25.5	26.4	67.2	21.3	72.2	17.6	21.8	25.4	58.5	23.4
CP06	The domestic robot blocks its own movement to physically prevent the camera from recording.	66.3	25.1	61.7	25.3	62.2	25.0	35.6	26.7	62.1	21.4	73.1	18.0	27.0	20.6	68.5	24.7
CP07	The domestic robot blocks its own movement to physically prevent the internet connection.	41.8	23.8	32.8	23.4	42.2	18.5	44.5	24.3	55.2	21.8	46.0	25.5	37.3	19.5	37.0	23.9
CP08	The domestic robot blocks its own movement to physically prevent the microphone from recording.	55.2	26.1	47.6	28.4	54.4	20.4	31.8	26.6	68.2	14.9	64.2	23.9	25.0	25.6	53.4	27.6
CP09	The domestic robot changes its posture to signal that the camera, microphone, and internet connection are deactivated.	49.2	27.4	43.2	30.5	50.4	24.8	36.3	25.4	61.2	22.4	59.1	25.9	33.6	22.7	48.6	26.7
CP10	The domestic robot covers its ears with its hands to physically prevent the microphone from recording.	21.9	26.9	17.2	23.3	26.2	30.1	42.7	29.0	81.2	18.6	57.8	31.8	37.2	31.3	34.2	28.7
CP11	The domestic robot covers its ears with its hands to signal that the microphone is off.	39.0	32.9	39.4	36.0	38.8	31.8	42.2	34.9	75.2	20.3	76.0	23.2	35.7	35.8	47.9	35.1
CP12	The domestic robot covers its eyes with its hands to physically prevent the camera from recording.	43.6	26.9	38.0	31.0	38.7	26.2	55.2	19.6	73.2	18.5	67.2	21.2	46.9	26.8	34.4	26.5
CP13	The domestic robot covers its eyes with its hands to signal that the camera is off.	46.9	28.9	32.9	19.6	46.9	22.2	34.4	30.7	69.7	28.2	73.8	27.6	23.8	25.4	52.0	26.7
CP14	The domestic robot crosses its arms to signal that it is disconnected from the internet.	72.7	9.3	62.8	21.9	68.0	17.3	30.7	21.8	76.4	14.4	81.0	15.0	21.2	21.4	68.9	20.5
CP15	The domestic robot deactivates its rotation function to physically prevent the camera from recording.	66.6	23.0	53.8	28.4	63.6	26.4	35.0	29.5	64.9	25.6	70.9	22.7	25.7	22.0	66.0	26.7
CP16	The domestic robot deactivates its rotation function to signal that the camera is off.	23.8	11.8	17.0	14.1	33.6	21.1	44.2	24.2	53.8	23.9	53.2	26.3	27.2	27.2	36.0	16.3
CP17	The domestic robot detaches its WiFi module to physically prevent the internet connection.	53.4	33.1	53.0	36.0	56.8	29.4	43.6	25.8	64.4	22.6	73.9	18.8	28.0	28.0	57.6	28.1
CP18	The domestic robot detaches its camera to physically prevent the camera from recording.	57.8	23.9	53.8	22.1	60.7	24.3	39.6	21.2	73.6	16.7	66.6	24.1	34.4	22.2	57.7	20.0
CP19	The domestic robot detaches its microphone to physically prevent the microphone from recording.	74.8	13.2	65.7	24.5	68.6	16.7	30.6	22.0	69.2	23.9	74.4	17.4	25.6	20.0	68.2	21.1
CP20	The domestic robot detaches its power source to physically prevent the camera, microphone, and internet connection from functioning.	52.7	30.5	39.6	34.6	47.0	30.8	39.4	29.5	62.8	27.1	72.0	27.5	28.6	29.9	48.3	33.9
CP21	The domestic robot displays a human gesture on its screen to signal that it is disconnected from the internet.	43.1	19.4	39.0	27.0	50.1	17.4	34.6	18.0	56.7	20.8	71.9	25.4	33.2	26.8	52.6	19.3
CP22	The domestic robot displays a human gesture on its screen to signal that the camera is off.	42.7	25.1	37.0	25.2	51.8	28.9	31.2	24.4	66.8	19.7	65.8	18.8	30.9	23.2	54.8	28.3
CP23	The domestic robot displays a human gesture on its screen to signal that the microphone is off.	38.9	25.1	40.6	29.2	45.6	24.4	43.2	24.2	61.1	15.3	66.7	15.7	29.6	27.7	49.9	25.4
CP24	The domestic robot displays a humanoid face that shuts its eyes on its screen to signal that the camera is off.	30.6	23.1	29.6	20.9	44.8	24.4	40.6	25.8	74.3	16.3	77.2	20.1	31.0	28.6	47.8	27.2
CP25	The domestic robot displays a symbol on its screen to signal that it is disconnected from the internet.	51.2	28.5	52.0	34.9	63.3	27.4	43.0	28.0	70.4	19.9	78.2	22.7	26.0	21.7	63.0	27.7
CP26	The domestic robot displays a symbol on its screen to signal that the camera is off.	47.4	32.6	39.8	32.9	53.2	31.4	37.6	27.4	71.0	19.9	78.4	20.2	33.0	26.7	53.2	30.7
CP27	The domestic robot displays a symbol on its screen to signal that the microphone is off.	60.6	25.3	54.0	33.8	57.2	25.6	35.3	21.4	64.7	20.6	74.0	22.5	25.8	24.5	69.6	26.0
CP28	The domestic robot displays text to signal that it is disconnected from the internet.	52.1	32.2	52.4	30.4	52.9	36.3	37.3	27.8	56.7	22.6	65.6	26.3	26.0	20.6	53.6	31.0
CP29	The domestic robot displays text to signal that the camera is off.	51.0	19.4	41.4	22.2	51.4	18.2	40.8	22.1	66.2	16.4	69.8	18.9	34.8	21.2	54.6	18.1
CP30	The domestic robot displays text to signal that the microphone is off.	55.2	29.2	44.9	31.3	62.6	22.6	32.2	27.5	67.2	20.8	80.8	14.3	25.0	24.0	61.6	27.1
CP31	The domestic robot displays the camera state on its screen to signal that the camera is off.	44.4	31.1	42.0	32.2	57.5	26.5	41.7	28.0	64.8	22.4	80.9	19.2	41.6	33.3	44.1	31.5
CP32	The domestic robot displays the connectivity state on the screen to signal that it is disconnected from the internet.	54.8	27.2	47.8	25.4	55.6	24.5	40.9	26.8	62.7	20.2	71.0	18.5	24.6	22.9	64.8	24.2
CP33	The domestic robot displays the microphone state on its screen to signal that the microphone is off.	56.2	28.3	54.3	33.7	54.7	28.4	28.5	22.7	64.8	18.8	75.2	14.5	27.7	23.2	62.4	26.0
CP34	The domestic robot enters physical confinement to physically prevent the camera, microphone, and internet connection from functioning.	58.7	30.3	57.0	30.2	61.5	24.2	40.8	29.5	74.4	21.6	66.6	24.0	30.0	27.1	54.5	27.0
CP35	The domestic robot faces the wall to physically prevent the camera from recording.	51.8	22.7	36.0	24.1	51.4	24.3	41.5	25.4	75.4	19.8	70.2	24.9	36.8	23.7	52.7	26.1
CP36	The domestic robot faces the wall to physically prevent the microphone from recording.	14.4	17.3	14.3	15.6	18.3	16.8	63.7	29.5	71.0	25.3	49.8	30.1	48.6	31.2	23.4	27.3
CP37	The domestic robot faces the wall to signal that the camera is off.	57.8	33.4	45.8	33.5	59.0	35.5	24.3	20.6	76.8	18.9	79.4	15.9	37.0	34.9	54.8	31.1
CP38	The domestic robot faces the wall to signal that the microphone is off.	27.8	22.3	23.4	24.7	33.0	27.1	47.2	24.0	66.6	22.0	58.0	26.9	36.8	27.5	33.6	17.0
CP39	The domestic robot goes to its docking station to physically prevent the camera, microphone, and internet connection from functioning.	70.6	19.3	59.1	25.7	65.9	18.4	39.2	28.3	63.7	26.8	69.1	24.1	28.3	26.0	69.4	20.4
CP40	The domestic robot has a fake antenna attached that illuminates to signal that it is disconnected from the internet.	54.0	26.4	51.8	21.8	56.4	25.4	51.1	22.4	66.7	19.8	69.0	22.8	28.6	19.6	61.8	17.8

Continued on next page

Table 1 – continued from previous page

Q	Communication Pattern	Pri.		T		E		I		N		U		D		Pref.	
		M	SD	M	SD	M	SD	M	SD	M	SD	M	SD	M	SD	M	SD
CP41	The domestic robot has a light band attached to signal that it is disconnected from the internet.	58.2	30.6	55.5	33.4	67.2	27.1	28.7	24.8	59.0	24.8	67.2	28.2	22.4	21.7	64.2	24.0
CP42	The domestic robot has a light band attached to signal that the camera is off.	54.6	26.1	55.8	31.4	62.0	20.0	36.8	26.3	67.4	20.5	72.0	18.7	22.6	25.7	65.2	21.5
CP43	The domestic robot has a light band attached to signal that the microphone is off.	47.8	32.1	39.2	30.3	44.1	27.0	43.8	30.3	75.8	15.9	73.8	24.3	20.3	20.4	61.3	25.8
CP44	The domestic robot imitates the human "shh" gesture/puts its finger in front of his mouth to signal that the microphone is off.	46.6	30.5	37.6	31.7	48.4	30.2	38.6	24.4	61.6	23.7	71.2	19.9	29.2	28.7	48.0	25.8
CP45	The domestic robot kills itself to physically prevent the camera, microphone, and internet connection from functioning.	49.0	34.6	57.9	25.6	44.9	33.3	51.4	32.2	74.6	19.3	44.6	32.4	65.9	38.5	33.9	36.5
CP46	The domestic robot parks itself against a pillow to physically prevent the microphone from recording.	15.0	13.6	14.8	16.6	21.6	18.3	49.6	29.4	74.6	22.4	53.8	29.7	45.3	29.5	27.8	25.4
CP47	The domestic robot plays distinct audio feedback to signal that it is disconnected from the internet.	41.2	31.4	41.2	31.9	50.6	30.6	55.0	29.6	72.2	21.2	70.2	25.5	31.6	29.1	51.2	29.4
CP48	The domestic robot plays distinct audio feedback to signal that the camera is off.	53.8	30.6	51.7	34.3	59.8	29.2	41.4	28.0	73.1	17.6	75.1	20.9	30.1	21.0	50.1	28.8
CP49	The domestic robot plays distinct audio feedback to signal that the microphone is off.	55.6	34.8	49.8	33.0	52.0	35.3	35.9	30.1	69.5	18.3	71.6	28.4	33.8	29.6	57.1	31.1
CP50	The domestic robot plays white noise to physically prevent the microphone from recording.	53.2	29.8	47.2	32.4	51.4	31.3	49.4	26.7	67.0	21.2	66.0	20.4	48.6	29.6	51.8	28.3
CP51	The domestic robot puts a physical cover over its camera to physically prevent the camera from recording.	80.5	17.1	62.8	29.7	73.5	26.0	27.4	20.5	76.9	19.6	76.6	22.7	22.2	21.4	75.4	25.0
CP52	The domestic robot puts a physical cover over its microphone to physically prevent the microphone from recording.	50.4	26.5	42.0	26.3	52.7	25.1	44.7	23.7	67.1	15.5	65.7	19.5	35.8	29.5	56.8	26.1
CP53	The domestic robot removes its head to physically prevent the camera, microphone, and internet connection from functioning.	48.5	32.1	42.6	30.4	49.8	31.4	52.4	24.3	79.4	18.5	61.6	30.4	50.6	29.3	45.8	24.2
CP54	The domestic robot removes the LAN cable to physically prevent the internet connection.	43.0	32.5	46.5	29.5	42.0	28.1	50.8	29.7	69.8	26.9	50.9	25.4	43.6	28.3	42.3	29.4
CP55	The domestic robot removes the camera's cable to physically prevent the camera from recording.	61.8	26.9	51.4	34.4	56.8	29.1	42.6	24.9	71.0	17.8	72.8	19.5	39.6	27.2	58.8	29.1
CP56	The domestic robot removes the microphone's cable to physically prevent the microphone from recording.	76.0	16.3	69.3	28.0	69.5	22.8	41.2	27.7	76.3	21.4	81.2	17.5	23.2	20.2	73.4	22.7
CP57	The domestic robot retracts its microphone to signal that the microphone is off.	52.0	29.8	38.0	26.9	53.2	26.7	35.2	30.4	70.1	22.8	69.5	23.9	30.4	30.1	48.0	30.4
CP58	The domestic robot shows you an empty connection plug to signal that it is disconnected from the internet.	43.8	30.0	37.8	32.3	55.8	32.5	33.4	23.7	63.6	21.7	70.0	30.4	25.4	25.5	61.0	27.4
CP59	The domestic robot shows you an empty connection plug to signal that the camera is off.	46.4	21.6	37.4	28.6	49.0	30.1	46.0	27.9	67.6	20.3	60.2	25.6	34.6	26.9	44.3	26.2
CP60	The domestic robot shows you an empty connection plug to signal that the microphone is off.	53.4	19.7	48.6	29.2	55.8	21.8	32.6	20.1	59.0	17.8	64.7	26.5	24.8	24.5	60.8	19.8
CP61	The domestic robot shows you the empty connection plug to physically prevent the camera from recording.	47.4	14.2	42.4	16.6	49.8	15.7	43.2	19.5	58.8	14.7	57.2	13.0	36.3	18.4	49.0	19.5
CP62	The domestic robot shows you the empty connection plug to physically prevent the microphone from recording.	53.0	26.9	51.2	27.3	58.0	25.3	44.1	25.9	65.8	21.4	69.1	26.1	28.4	27.1	61.8	27.0
CP63	The domestic robot transforms into a different shape to signal that the camera, microphone, and internet connection are deactivated.	53.4	29.3	48.1	29.1	58.3	25.6	40.6	27.6	77.0	18.3	68.2	28.4	35.3	28.5	52.3	28.8
CP64	The domestic robot turns its camera away to physically prevent the camera from recording.	48.6	31.5	43.0	31.9	49.8	28.7	45.5	23.5	70.0	18.5	71.6	19.1	41.6	29.1	54.0	29.8
CP65	The domestic robot turns off its screen to signal that the camera, microphone, and internet connection are deactivated.	47.4	26.2	35.5	27.3	48.2	28.9	31.4	21.5	63.2	17.4	70.0	17.7	20.0	18.2	47.4	24.5
CP66	The domestic robot uses a hand gesture to signal that it is disconnected from the internet.	51.4	30.4	50.0	35.7	56.9	28.1	30.1	28.6	61.2	28.3	71.4	18.5	13.5	14.7	55.8	28.3
CP67	The domestic robot uses a hand gesture to signal that the camera is off.	40.9	30.3	43.2	31.7	49.8	29.1	27.5	24.0	55.1	27.3	56.2	25.3	18.6	19.4	47.4	30.3
CP68	The domestic robot uses a hand gesture to signal that the microphone is off.	64.4	24.8	55.5	27.1	60.6	26.0	36.8	29.9	69.2	23.1	70.8	28.3	15.5	12.4	62.9	28.2
CP69	The domestic robot uses a physical switch to physically prevent the camera from recording.	72.2	16.7	66.4	25.8	70.2	27.5	44.0	31.4	69.7	24.6	76.0	23.3	26.8	24.7	68.2	24.9
CP70	The domestic robot uses a physical switch to physically prevent the internet connection.	55.1	25.4	55.2	28.3	55.1	28.6	40.6	22.6	67.0	16.3	70.1	19.8	35.2	27.0	61.9	21.2
CP71	The domestic robot uses a physical switch to physically prevent the microphone from recording.	50.8	28.5	49.8	29.0	46.2	26.0	34.9	19.3	60.8	22.5	70.5	21.3	28.5	24.4	60.6	28.7
CP72	The domestic robot uses its voice to signal that it is disconnected from the internet.	44.8	29.0	40.4	31.6	55.2	26.1	42.2	23.5	70.7	14.3	76.2	19.2	37.8	27.0	52.3	25.0
CP73	The domestic robot uses its voice to signal that the camera is off.	37.2	27.0	33.2	27.3	38.8	31.1	44.6	25.8	67.4	19.3	73.8	20.4	33.2	27.1	44.6	30.6
CP74	The domestic robot uses its voice to signal that the microphone is off.	50.4	26.3	45.4	28.4	57.0	26.1	40.0	27.2	59.9	27.2	76.8	22.3	32.6	22.1	52.6	27.0
CP75	The domestic robot uses light feedback to signal that it is disconnected from the internet.	47.6	34.4	38.8	31.9	47.9	33.6	31.6	25.2	58.9	27.5	62.2	29.9	29.8	26.4	56.2	34.9
CP76	The domestic robot uses light feedback to signal that the camera is off.	43.6	21.4	40.0	22.9	48.8	26.1	52.4	25.9	61.3	23.8	67.2	25.1	37.0	22.8	47.1	23.2
CP77	The domestic robot uses light feedback to signal that the microphone is off.	54.4	27.3	50.4	28.2	56.6	26.5	29.2	24.2	60.7	23.5	73.4	22.8	19.5	23.7	56.4	27.8
CP78	The domestic robot uses projection to signal that it is disconnected from the internet.	48.8	25.9	49.4	28.8	59.0	28.7	38.0	28.7	63.0	28.3	67.8	24.1	25.6	23.6	60.8	20.9
CP79	The domestic robot uses projection to signal that the camera is off.	54.3	29.1	49.8	25.8	53.6	30.0	31.7	27.2	66.3	23.9	68.5	21.8	24.2	18.1	49.2	28.3
CP80	The domestic robot uses projection to signal that the microphone is off.	63.4	21.9	47.0	27.2	62.5	21.8	37.6	19.5	66.6	16.1	65.7	19.3	35.7	23.8	61.2	22.6
CP81	The domestic robot uses the smart lights in your home to signal that it is disconnected from the internet.	59.0	30.8	53.2	33.4	61.5	26.8	47.5	30.1	74.5	25.3	73.4	26.1	31.9	31.2	61.8	28.1
CP82	The domestic robot uses the smart lights in your home to signal that the camera is off.	38.8	23.9	35.2	21.9	40.2	26.3	47.6	23.6	60.0	23.6	52.0	25.7	44.6	21.4	40.0	26.0
CP83	The domestic robot uses the smart lights in your home to signal that the microphone is off.	58.2	32.4	48.2	33.9	54.6	28.7	41.0	31.8	66.6	26.9	69.9	27.5	28.8	29.0	52.2	29.1
CP84	The domestic robot waves a banner to signal that it is disconnected from the internet.	45.0	27.0	42.7	27.8	48.0	29.4	36.9	22.0	74.0	18.6	69.8	22.8	33.4	21.7	43.5	23.5
CP85	The domestic robot waves a banner to signal that the camera is off.	61.8	22.4	48.2	24.4	62.2	22.6	37.9	22.7	64.6	27.1	71.4	22.4	27.3	22.7	52.8	26.3
CP86	The domestic robot waves a banner to signal that the microphone is off.	45.8	23.6	42.9	25.3	45.9	21.5	39.2	22.0	59.6	21.3	74.0	14.1	31.0	30.0	45.6	21.1

A.3 Survey on Communication Patterns

Immerse yourself in the following situation: You have a domestic robot at home that provides entertainment and supports you with daily chores. While you appreciate the domestic robot for the convenience it provides, in some cases, you want privacy. For that, the robot uses a communication pattern to show you that your privacy is protected. Your robot does the following: *[Communication pattern.]* Please indicate to which extent you agree with the following statements:

1. This communication pattern protects my privacy very well. (Slider)
2. When the robot uses this communication pattern, I very much trust that the functionality is deactivated. (Slider)
3. This communication pattern is very effective. (Slider)
4. This communication pattern is very intrusive. (Slider)
5. This communication pattern is very noticeable. (Slider)
6. This communication pattern is very understandable. (Slider)
7. Put the slider all the way to the right side. (Attention check)
8. This communication pattern is very disturbing. (Slider)
9. I very much like my domestic robot to use this communication pattern. (Slider)
10. If you have any additional feedback, please let us know here. (Free text)

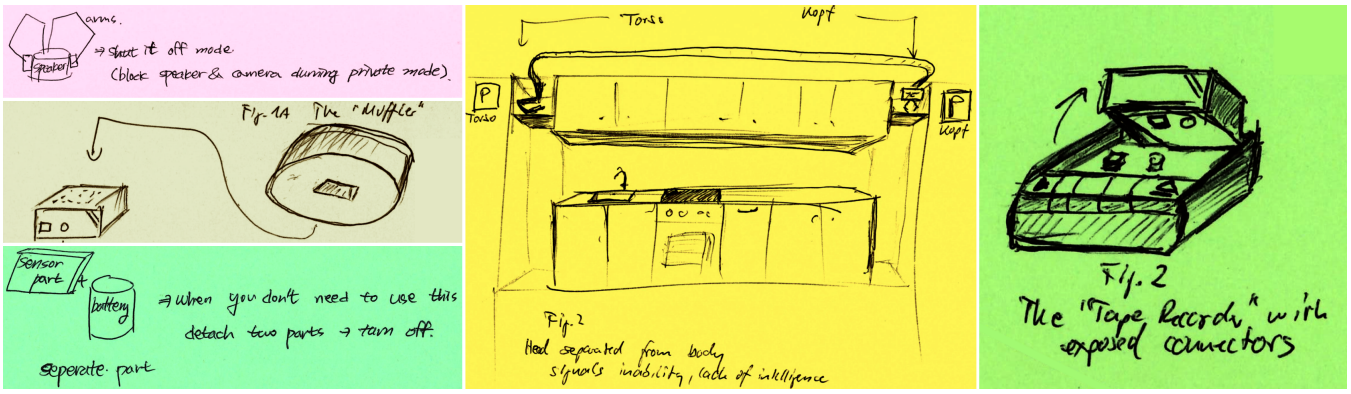


Figure 4: Examples of sketches our participants created in the focus groups.