Reimagining Consent Through Embodied Cognition: Supporting Users' Privacy Understanding in Humanoid Social Robots

Leah Zhang-Kennedy
University of Waterloo
lzhangkennedy@uwaterloo.ca

JaeEun Jen Shin
University of Waterloo
jeshin@uwaterloo.ca

Yue Hu
University of Waterloo
yue.hu@uwaterloo.ca

Abstract

Social robots are increasingly being developed to support users' physical, cognitive, and social well-being in domestic and care environments. However, their embodied, socially interactive, and mobile nature introduces privacy challenges that are not well addressed by current screen-based privacy notice and consent paradigms. In this position paper, we argue for embodied privacy mechanisms grounded in embodied cognition, where privacy interactions become tangible, observable, and socially meaningful actions. We outline several approaches, including tangible privacy tokens, gesture-based sensor modulation, configurable sensor covers, and spatial or proximity-based privacy controls. We further discuss how these mechanisms may particularly benefit children and older adults, whose needs are often poorly supported by conventional privacy interfaces. Finally, we present preliminary findings from an in-home co-design study with children to support our argument and discuss future work.

1 Introduction

Social robots have the potential to deliver physical, cognitive, and social support, along with health-related support, in homes and in care settings. However, their ability to collect and process vast amounts of personal data, such as video, audio, touch, gestures, facial recognition, emotional assessments, and environmental information, has raised significant privacy concerns, hindering their acceptance and adoption [7, 8].

The advanced interaction capabilities of social robots, combined with their ability to foster social relationships, introduce unique threats to users' psychological, social, and physical privacy [6–8]. Humanoid social robots (HSRs), in particular, communicate through human-like social cues and embodied behaviors that can foster trust, emotional attachment, and greater willingness to disclose personal information [14, 18]. Their human-like appearance and behaviors may also lead users to anthropomorphize the robot, attributing human qualities, intentions, and social status, potentially causing users to overestimate the robot's understanding and capabilities while underestimating its technical limitations and data collection practices [9].

Researchers suggest that robots should clearly communicate their privacy states to users [7, 20]. However, designing privacy controls and consent mechanisms that provide accessible, comprehensive, and meaningful choices in HSR contexts is under-explored. HSRs possess advanced interaction capabilities and multimodal sensing infrastructures that differ substantially from the interaction paradigms underlying current privacy notice and consent mechanisms used in mobile, web, and Internet of Things (IoT) technologies [2, 7].

Unlike conventional IoT devices, HSRs are physically embodied, socially interactive, and mobile agents that actively move through and engage with users' environments. While many IoT devices remain stationary and operate in the background, HSRs communicate through speech, gestures, gaze, touch, and locomotion, creating stronger perceptions of social presence and agency. Their ability to autonomously navigate domestic spaces introduces unique privacy concerns, as robots may enter sensitive areas, reposition themselves to observe interactions, or collect information across multiple contexts within the home. As a result, privacy interactions with HSRs are not limited to static device settings, but become ongoing, embodied, and socially negotiated experiences that unfold through movement and interaction in physical spaces.

Current privacy consent models are largely screen-based, making them difficult to implement on HSRs that lack traditional display interfaces. Current solutions are usually decoupled from the main system and provided as text-based privacy policies on companion mobile devices and websites,

USENIX Symposium on Usable Privacy and Security (SOUPS) 2026.
August 23–26, 2026, Hannover, Germany.

while the robot itself does not provide any privacy controls. As a result, users are less likely to read the notice and therefore may not realize that their expectations do not match the robots' actual data practices. To address these issues, previous research highlights the need to develop privacy notices through the robots' available communication channels and interaction capabilities [20].

In this position paper, we discuss the need for a systematic understanding of effective privacy notices and the design of real-time control mechanisms within these systems. Here, we conceptualize "consent" and "privacy choice" in a design context—not as legal definitions, but as the capabilities provided by digital systems that enable users to understand and control how their personal data is recorded, stored, and shared. The design of privacy notice and consent mechanisms should include considerations of social norms (e.g., robot disabling its camera in private or sensitive spaces), appropriate data flows (e.g., sharing specific information between the robot, children, parents, caregivers, educators, or healthcare providers) and ethical implications of HSR use (e.g., active and passive monitoring of children and older adults). Specifically, we advocate for developing and evaluating embodied privacy notices and consent mechanisms to assess whether they are understandable and accessible, foster trust and transparency, and provide meaningful privacy controls, particularly for vulnerable populations like children and older adults.

2 Embodied Privacy Mechanisms

Drawing on embodied cognition, a theoretical framework that emphasizes how cognitive processes are grounded in the body's sensory and motor systems and shaped by physical action and interaction with the environment [13], we argue that privacy and security interactions should move beyond text-based interfaces toward tangible and physically interactive mechanisms that are more intuitive, accessible, and meaningful for users.

Extensive research in psychology, human-computer interaction (HCI), and learning sciences suggests that, from an early age, humans often develop an understanding of abstract concepts through physical and tangible experiences before engaging with more symbolic or abstract representations (e.g., [1]). Drawing on this perspective, we envision HSR-mediated systems that make privacy choices both tangible and meaningful through on-robot notice and consent mechanisms that combine speech, sensory feedback, and tangible interaction cues to communicate privacy-related information to users. Rather than relying exclusively on menus, settings pages, or text-based consent notifications, these mechanisms externalize privacy interactions into observable physical actions that users can directly manipulate, interpret, and negotiate. Such embodied interactions can better align with the preferred modes of interaction while also shaping how users perceive, understand, and engage with privacy-related decisions [17].

As proof-of-concept examples, we propose several imagined directions for embodied privacy mechanisms in HSRs.

2.1 Tangible Privacy Tokens

One potential direction is the use of physical artifacts, such as tangible privacy tokens embedded with radio-frequency identification (RFID), which users could insert or remove from the robot to signal consent, refusal, or sharing preferences. For example, placing a green camera token in a robot's slot to allow recording or sharing, and a red token to deny or stop it. Different tokens could also correspond to different privacy states, sensing capabilities, or sharing destinations.

The purpose of these interactions is to make privacy visible, accessible, and actionable by ensuring that physical actions of users have a clear and enforceable effect on robot behaviors. Tangible interfaces provide persistent physical representations of digital states and interactions, enabling users to more readily perceive, interpret, and act on privacy-related information [3]. In this way, tokens function not only as control mechanisms, but also as communicative artifacts that externalize otherwise invisible data practices.

2.2 Gesture-Based Sensor Modulation

Beyond discrete physical artifacts, embodied privacy interactions may also emerge through natural gestures, touch, and direct manipulation of robot sensors. One direction we envision is sensor modulation enabled through intuitive bodily actions that temporarily disable or reconfigure sensing capabilities. For example, users covering a robot's "eyes" (camera) or "ears" (microphone) with their hands could signal the robot to stop data collection, with the action confirmed through multimodal feedback such as lights, sounds, or speech.

To further support transparency, these embodied interactions could be paired with destination-specific cues that communicate how information is being shared. For example, robots might use distinct lighting patterns, directional gestures, or tangible markers associated with particular recipients or destinations to indicate where data is being transmitted. These cues help users not only control sensing and recording, but also understand the flow of their information and ground privacy decisions in socially meaningful interactions.

2.3 Configurable Physical Covers or Shutters

Embodied sensor control could also extend to configurable physical covers or shutters integrated directly into the robot's design. Users could physically slide, rotate, detach, or attach modular covers over specific sensors to selectively limit sensing capabilities. Unlike software-based toggles hidden within menus or settings interfaces, these mechanisms provide immediate and visible confirmation that sensing functions have been altered. This visibility may be particularly valuable in shared or multi-user environments, where privacy states need to be legible not only to the primary user, but also to bystanders and co-located individuals. For example, a visibly covered camera or physically closed microphone shutters can communicate privacy boundaries in ways that are socially observable [12]. Such mechanisms may also foster greater trust and accountability by reducing ambiguity around whether sensing systems are active.

2.4 Spatial/Proximity-Based Privacy Controls

A fourth direction involves spatial and proximity-based privacy controls, where users regulate privacy through their physical location, orientation, or movement relative to the robot. For example, moving a robot into designated "private zones" within a room, turning the robot away during sensitive moments, or stepping outside a predefined interaction boundary could automatically limit sensing, recording, or data sharing.

These interactions leverage intuitive spatial behaviors already embedded within everyday social practices. Humans routinely use space, orientation, and distance to negotiate social boundaries, attention, and intimacy. Embodied privacy mechanisms could similarly use these existing behaviors as natural cues for regulating data practices. Rather than explicitly requiring users to configure settings, privacy preferences could emerge implicitly through movement and spatial interaction to adapt to transitions between public, semi-private, and private contexts.

3 Users and Usage Contexts

While we imagine embodied privacy mechanisms as broadly beneficial for users, we believe they may be particularly valuable for populations whose cognitive, attentional, sensory, or developmental needs are not well supported by conventional screen-based privacy interfaces. In particular, we argue that these systems may be especially valuable for two user groups whose needs are often insufficiently supported by conventional privacy interfaces: children and older adults.

3.1 Children

Research on children's understanding of digital privacy suggests that children initially grasp privacy through ownership and control of tangible objects (e.g., "this toy is mine") before extending these ideas toward more abstract and intangible concepts such as personal information and data ownership ("my data belongs to me") [4, 22]. However, many current privacy systems remain heavily screen-based, text-centric, and abstract, making them developmentally inappropriate for children whose understanding of privacy emerges gradually through concrete and socially situated experiences [16,22,23]. HSRs offer a unique opportunity to make privacy choices easier to understand by leveraging children's natural interactions with physical objects, social agents, and sensory feedback in their environments.

While embodied privacy interfaces may benefit children broadly, they may be particularly valuable for children with neurodevelopmental conditions, such as Attention-Deficit/Hyperactivity Disorder (ADHD) and autism spectrum disorder (ASD). Children with ADHD may experience difficulties with executive functioning skills, including working memory, attention, and self-regulation [19], which may hinder their ability to consistently monitor, recall, and act on privacy choices [10]. Similarly, children with ASD often show weaker theory of mind [11], including the ability to realize that others only know what is shared with them, which may affect how they understand and manage their privacy. Although the direct link between these cognitive traits and privacy comprehension has not been systematically studied (a gap future research could address), early evidence from studies of autistic teenagers' online practices showed differences in their privacy attitudes and behaviors compared to neurotypical peers [10]. We therefore hypothesize that neurodivergent children may also engage differently with privacy choices in HSR contexts. These considerations are especially important given the growing use of HSRs in educational, therapeutic, and assistive interventions for children. As such, developing privacy mechanisms that accommodate diverse attentional profiles, sensory sensitivities, communication styles, and cognitive needs is promising direction for future research.

3.2 Older Adults

As HSRs become increasingly integrated into aging and healthcare infrastructures, there is a growing need for privacy mechanisms and design guidelines that account for older adults' diverse cognitive, sensory, physical, and social needs. HSRs promise to provide physical, cognitive, and social support, as well as health-related interventions for older adults in both home and care settings to support aging in place, reduce caregiver burden, provide companionship, and mitigate loneliness and social isolation [15].

At the same time, the capabilities that make HSRs potentially valuable for older adults also introduce significant privacy concerns. These robots often rely on continuous sensing and data collection [15], and such forms of monitoring may be particularly sensitive in private and healthcare settings [5]. These concerns are especially important because older adults are frequently framed as a vulnerable population within healthcare and assistive technology contexts [21]. Furthermore, age-related changes in cognition, memory, vision, hearing, or digital literacy may make conventional screen-based privacy notices and consent mechanisms difficult to navigate and interpret. Privacy decisions in care settings are often negotiated among multiple stakeholders [15], including family members, caregivers, healthcare providers, and institutional staff, creating additional complexity around consent, autonomy, and information sharing. As a result, existing approaches to privacy management may inadequately support older adults in understanding and meaningfully controlling how HSR systems operate in their everyday lives. The proposed embodied privacy mechanisms could provide older adults with more immediate and legible ways to regulate sensing and data collection without requiring complex menu navigation or abstract configuration settings. Similarly, privacy states could be more visible to caregivers, family members, and co-located individuals, helping to establish shared understandings of when sensing systems are active or inactive.

4 Preliminary Findings

This paper presents initial ideas for establishing a broader research agenda for embodied privacy-enhancing technologies in HSRs. To inform this research, we conducted an REB-approved, two-session in-home co-design study with 20 children aged 7–12 years and their parents. Families were recruited through social media and snowball sampling. Written informed consent was obtained from legal guardians, and children provided assent before participation. The first session (approximately 60 minutes) included a robot demonstration using NAO, a small humanoid robot, introduction to privacy concepts, and a card-sorting activity to enable children to explore preferences for privacy notice placement, communication modality, and notice characteristics (e.g., colors). Parents also completed a demographic questionnaire. The second session (60–90 minutes) involved a participatory drawing activity in which children designed privacy notices for the robot, building on their preferences identified during the first session. This was followed by semi-structured interviews with both children and parents. All sessions were video and audio-recorded, transcribed, and analyzed using thematic analysis. Families received $50 CAD in compensation.

Our preliminary findings suggest that children indeed conceptualize privacy interactions with HSRs as embodied and socially situated experiences rather than purely functional system notifications. Participants consistently preferred multimodal and on-robot privacy cues, particularly LED lights, dialogue, gestures, and poses that mapped to the robot's physical body and sensing capabilities. For example, children associated privacy states with specific body regions (e.g., eyes for cameras and ears for microphones) and expected robots to communicate sensing activities through socially meaningful behaviors, such as verbal announcements, listening poses, and permission-seeking interactions.

However, our findings also revealed developmental differences in privacy expectations. Pre-adolescent children (e.g., aged 7 to 9) demonstrated stronger preferences for embodied and anthropomorphic interactions, such as gestures and poses, whereas older children and parents preferred more explicit and functionally grounded notice styles, including lights and spoken dialogue. These findings suggest that embodied privacy notices may be particularly effective for younger children, who may engage more naturally with socially expressive and physically interactive forms of communication.

5 Conclusion and Future Work

In this position paper, we argued that existing screen-based privacy notice and consent paradigms are insufficient for HSRs, whose embodied, mobile, and socially interactive nature introduces new privacy challenges that unfold through ongoing interaction in physical environments. Drawing on embodied cognition, we proposed a shift toward embodied privacy mechanisms that externalize privacy interactions into tangible, observable, and socially meaningful actions. We outlined several possible directions, and further argued that these mechanisms may be particularly beneficial for children and older adults, whose needs are often poorly supported by conventional privacy interfaces. We have presented preliminary findings from a co-design study with families that provided early empirical support for some of the concepts proposed in this paper.

As future work, we plan to design, prototype, and evaluate the embodied privacy mechanisms proposed in this paper, examining how well these approaches support users' understanding, trust, consent behavior, and sense of control in real-world settings. More broadly, we hope this work encourages interdisciplinary research at the intersection of human-robot interaction, usable privacy and security, accessibility, and embodied interaction design.

References

[1] Moyosore Ale, Miriam Sturdee, and Elisa Rubegni. A systematic survey on embodied cognition: 11 years of research in child–computer interaction. *International Journal of Child-Computer Interaction*, 33:100478, 2022.

[2] Anna Chatzimichali, Ross Harrison, and Dimitrios Chrysostomou. Toward privacy-sensitive human–robot interaction: Privacy terms and human–data interaction in the personal robot era. *Paladyn, Journal of Behavioral Robotics*, 12(1):160–174, 2020.

[3] Sarah Delgado Rodriguez, Maximiliane Windl, Florian Alt, and Karola Marky. The TaPSI research framework – a systematization of knowledge on tangible privacy and security interfaces. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, pages 1–28, 2025.

[4] Susan A Gelman, Shaylene E Nancekivell, Young-eun Lee, and Florian Schaub. Children's understanding of digital tracking and digital privacy. *Handbook of Children and Screens: Digital Media, Development, and Well-Being from Birth Through Adolescence*, pages 643–649, 2024.

[5] Erin E Harrington, Alex J Bishop, Ha M Do, and Weihua Sheng. Perceptions of socially assistive robots: a pilot study exploring older adults' concerns. *Current Psychology*, 42(3):2145–2156, 2023.

[6] Min Kyung Lee, Karen P Tang, Jodi Forlizzi, and Sara Kiesler. Understanding users' perception of privacy in human-robot interaction. In *Proceedings of the 6th international conference on Human-robot interaction*, pages 181–182, 2011.

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

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

[9] Bertram Malle, Kerstin Fischer, James Young, Ajung Moon, and Emily Collins. Trust and the discrepancy between expectations and actual capabilities of social robots. In *Human-robot interaction: Control, analysis, and design*, pages 1–23. Cambridge Scholars Press, 2020.

[10] Jessica N Rocheleau and Sonia Chiasson. Privacy and safety on social networking sites: autistic and non-autistic teenagers' attitudes and behaviors. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 29(1):1–39, 2022.

[11] Belen Rosello, Carmen Berenguer, Inmaculada Baixauli, Rosa García, and Ana Miranda. Theory of mind profiles in children with autism spectrum disorder: Adaptive/social skills and pragmatic competence. *Frontiers in Psychology*, 11:567401, 2020.

[12] Sujay Shalawadi, Christopher Getschmann, Niels van Berkel, and Florian Echtler. Manual, hybrid, and automatic privacy covers for smart home cameras. In *Proceedings of the 2024 ACM Designing Interactive Systems Conference*, pages 3453–3470, 2024.

[13] Lawrence Shapiro. *Embodied cognition*. Routledge, 2019.

[14] JaeEun Jen Shin, Amr Hamdi, An Bella Chen, Yue Hu, and Leah Zhang-Kennedy. Toward safe child-robot interactions: Exploring children's and parents' privacy perceptions of humanoid social robots. In *International Conference on Social Robotics*, pages 253–272. Springer, 2025.

[15] Andrea Slane and Isabel Pedersen. Older people's perspectives on privacy, surveillance and consumer socially assistive robots: Paradoxes, trade-offs and the future of privacy protection. *Surveillance and Consumer Socially Assistive Robots: Paradoxes, Trade-offs and the Future of Privacy Protection (June 14, 2023)*, 2023.

[16] Mariya Stoilova, Rishita Nandagiri, and Sonia Livingstone. Children's understanding of personal data and privacy online–a systematic evidence mapping. *Information, Communication & Society*, 24(4):557–575, 2021.

[17] Peng Su and Xiang Yuan. Are you watching me? a study on privacy notice design of social robot. In *International Conference on Applied Human Factors and Ergonomics*, pages 339–344. Springer, 2021.

[18] 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 *International Conference on Social Robotics*, pages 506–515. Springer, 2017.

[19] Parker Townes, Chunlin Liu, Prabdeep Panesar, Daniel Devoe, Soo Youn Lee, Gracie Taylor, Paul D Arnold, Jennifer Crosbie, and Russell Schachar. Do ASD and ADHD have distinct executive function deficits? a systematic review and meta-analysis of direct comparison studies. *Journal of Attention Disorders*, 27(14):1571–1582, 2023.

[20] Maximiliane Windl, Jan Leusmann, Albrecht Schmidt, Sebastian S Feger, and Sven Mayer. Privacy communication patterns for domestic robots. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*, pages 121–138, 2024.

[21] Tammy Worth. Are robots the solution to the crisis in older-person care? *Nature*, 2024.

[22] Leah Zhang-Kennedy, Christine Mekhail, Yomna Abdelaziz, and Sonia Chiasson. From nosy little brothers to stranger-danger: Children and parents' perception of mobile threats. In *Proceedings of the The 15th International Conference on Interaction Design and Children*, pages 388–399, 2016.

[23] Jun Zhao, Ge Wang, Carys Dally, Petr Slovak, Julian Edbrooke-Childs, Max Van Kleek, and Nigel Shadbolt. I make up a silly name' understanding children's perception of privacy risks online. In *Proceedings of the 2019 CHI conference on human factors in computing systems*, pages 1–13, 2019.