Exploring Privacy Implications for Domestic Robot Mediators

Manuel Dietrich, Thomas Weisswange

2022

Preprint:

This is an accepted article published in IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS 2022) - Workshop on Robot Trust for Symbiotic Societies (RTSS 2022). The final authenticated version is available online at: https://doi.org/[DOI not available]

Exploring Privacy Implications for Domestic Robot Mediators

Manuel Dietrich, Thomas H. Weisswange

***Abstract*— To become part of our everyday social environment, robots will need to be developed in a way to gain an appropriate level of trust of humans, both users and bystanders. One important aspect influencing trust is the handling of privacy. In this paper, we explore privacy challenges of social robots when acting in the role of mediators in human-human interactions within domestic assistance scenarios. We approach this topic by reviewing privacy research on related technologies that already exist in many households, namely smart home and smart speaker devices. We extract common user concerns and requirements with respect to general data sharing based on their experience with using these technologies and evaluate which of these will be relevant for a robotic mediator design. We also discuss research on privacy implications of shared devices and telepresence robots, which extend the use cases to possible data sharing between humans. Finally, we point out mediator-specific privacy challenges in the realm of social privacy to highlight open research questions that should be addressed when targeting a deployment of robotic mediators.**

I. Introduction

Social robots are a class of autonomous artificial agents that support humans in everyday life. Natural communication, verbal or non-verbal, as well as the understanding of human behavior in a cognitive and emotional sense (e.g., through affective computing) have been proposed as key capabilities for a successful human-robot relationships [1]. Beyond the support of individual humans, social robots are also increasingly designed to play a role in activities and communications been individuals or groups of people [2]. Examples are team activities where the robot can support the users to achieve a common goal, to resolve conflicts and improve communication quality [3]–[6]. In extension, robots that take a pro-active role to shape inter-person relationships and cooperative activities may be referred to as embodied mediators [7].

Any social robot will likely need to use a variety of data about individuals to be able to perform its functionality. This might, for instance, include video or audio footage, more high-level information such as past interactions, the locations of objects, and even a user's preferences and mental states. Using such knowledge about individuals can be of particular interest for mediation to advance cooperation, for instance to inform a group about one partner's limitation (e.g., high workload) or to highlight mutual interests.

Researchers started to investigate effects of such personal data usage for the evaluation of interactions between users and robots (e.g., [8]). However, in many cases, this is restricted to traditional challenges of 'data protection' such as those addressed in legal frameworks like the European General Data Protection Regulation [9] or the California Consumer Privacy Act [10] and privacy threats due to inappropriate use of personal data by (robot-)service providers [11]. One aspect which has been also looked at, is how embodiment impacts a users' privacy perception. Tonkin et al [12] found that when data collection was preformed through an embodied agent instead of an abstract sensor, people were more comfortable with it (similar results were found in [13]).

When looking at social robots that address inter-human relationships like robot mediators, it might be important for a privacy design to go beyond these traditional topics. It becomes relevant, to also discuss how users can govern their personal data, which might be disclosed to other users or bystanders ("Social privacy") within normal operation. We know from inter-human privacy theories that a wrongly directed information flow can greatly impact human wellbeing, for instance causes feelings of exposure and loss of control or fear of being stigmatized or losing their face (e.g., Communication Privacy Management (CPM) theory [14]).

Following the privacy-by-design paradigm [11], [15], we argue that it is important to consider privacy from an early stage in system development. For example, in prior work we discussed why and how assistant robot should be designed to allow a dynamic management of privacy configurations [16]. To approach privacy for robotic mediators, one needs to first map the range of different relevant aspects and evaluate potentially existing approaches that might already be used in related technologies. From prior research, we also know that social privacy expectations can differ a lot depending on the context and application [17]. Here our focus lies on robotic mediation in a domestic setting as a promising application area with high social privacy implications.

In this perspective paper, we look at research work studying users' privacy expectations and concerns with smart speaker and IoT devices as well as classical social robotics technologies that people have applied in a home context. This further leads into a discussion about what might be additional privacy-related aspects and where further research will be required before releasing a robotic mediator to general users. Prior to that, we will introduce some examples of robot mediators that have been proposed to improve the wellbeing of their owners, not (only) through being companions but through facilitating human-human interactions.

II. Domestic Social robotic mediators

Social or socially assistive robots are in general seen as promising technology to enhance people's health and wellbeing in everyday domestic settings. When serving as personalized coaches or companions, they could be shown to have positive psychological effects on individuals, either through social presence [18], reactive behavior [19], mental assistance [20], as well as by providing positive interventions fostering self-awareness and gratitude, as, for instance, demonstrated for a student dormitory robot [21].

On the other hand, it was proposed that social robots can also increase wellbeing not only by being a personal interaction partner but by acting as an enabler for social relations and mutual support between people. Chita-Tegmark & Schuetz

M.D. & T.H.W. are with Honda Research Institute Europe GmbH, Germany (e-mail: firstname.lastname@honda-ri.de).

[22] have systematically analyzed the literature about social robots and highlighted opportunities for robots as social mediators. Domestic robot mediators are described as entities which support people living together or help to enable or maintain relationships with outsiders (family and friends) [22]. Such robot can act as an explicit group member [23] but also by more subtly influencing interaction dynamics [24], [25] or even by providing explicit means to start [26] or enhance a remote connection [27]–[30].

Based on their discussion, social robotic mediators can be characterized as follows: First, they primary support multi-human constellations rather than focusing on a single human interaction partner, which has been the typical setup for personalized coaches and companions (in line with a recent trend towards human-human-robot interaction design, e.g., [2], [31]). Second, they do so by taking a role as facilitator to enable valued social activities, maintain rewarding relationships or mutual support [32]. Third, as robotic agents, they operate with a certain degree of agency. For instance, a robot mediator is able to pro-actively intervene or react according to how a social situation evolves based on environmental sensing. This separates them from the 'assistance on demand' paradigm of smart speaker applications or classic service-oriented robots.

As an example, we want to go beyond what is already discussed in the use cases above. Let us imagine a domestic robot mediator which provides support for an elderly woman living alone at home. Such a robot could assist with everyday tasks like answering questions, chatting, setting reminders, or providing bring-and-fetch services. As a mediator, the robot is not only providing one-on-one support, but also has the dedicated task to proactively involve others to improve the owner's life. Let us suppose that the robot has information about the fact that the elderly woman was looking for her blood measure monitor but could not find it. When her daughter is visiting the next time, a mediation event could be triggered, where the robot verbalizes that her mother could not find her blood measure monitor and encourages the daughter to support searching for the monitor. Mediation of such kind implies many challenges, such as timing, topic selection and context-awareness, but also what and if information should be disclosed to involve others.

III. LITERATURE REVIEW

In this section, we will look at privacy concerns and expectations which users of related technologies have reported in user-experience studies. Smart speakers, smart home and IoT devices are of particular interest as due to their general public availability, insights are grounded on real world user experience [33]–[36]. Furthermore, robotic mediators will likely share some of the sensing and processing capabilities with these technologies and therefor likely have overlapping privacy aspects. After that, we will also investigate existing work with telerobots and social companion robots to potentially identify concepts that cover the specific implications of an embodiment.

TABLE I.

Papers	N	Devices / Technologies	Data collection	Experience
[37]	23	Google Home, Amazon Echo	Phone or WhatsApp call interviews	Owners and frequent users
[35]	8	Nest Learning Thermostat, Amazon Echo, Samsung SmartThings Hub, etc.	Skype call interviews	Owners and frequent users
[36]	26	Google Home, Amazon Echo, Apple HomePod, etc.	Semi-structured in-person interviews	Owners and frequent users
[38]	15	Samsung SmartThings, Amazon Echo, Philips Hue etc.	Phone or Skype call interviews	Owners and frequent users
[39]	81	Remote controlled cleaning robot ("Fetch")	Online survey (with videos showing scenarios)	No particular experience
[40]	13	Tele-maid, Beam+ telepresence system, roboreceptionist	Focus groups discussion (stimuli videos / demo)	No particular experience
[41]	6	Health robots, household robots, Robots for children, Educational robots	Phone interviews with open questions	Experts (university, legal, industry)
[42]	12	PeopleBot TM (ActivMedia Robotics)	Interviews (after being exposed to a real robot using personal data)	Recruited from a parallel long-term HRI study
[43]	54	Voice activated personal agents with pro-active functionalities.	At home interviews (based on storyboards)	~90% had experience with smart speakers

a. Studies exploring privacy perceptions of robot mediator related intelligent home technologies

A. *Smart home, IoT and smart speaker realm*

Looking into privacy effects of smart speakers like the Amazon Echo or Google Home but also other smart home devices like the Nest thermostat, Tabassum and colleagues [37] and Zheng and colleagues [35] conducted interviews with regular owners of such devices. Results reported by Tabassum et al. [37] show that data storage is an area with high uncertainties in understanding, although most participants were aware that significant amounts of data were stored outside of their homes and devices. Many potential threats that have been mentioned relate to data leakage and exploitation by unknown third parties, but many participants also admitted that they do not implement existing mitigation strategies due to complexity of the user interface of such solutions. Interestingly, both studies ([35], [37]) reported that raw audio and video data were considered as extremely sensitive even though most participants were not aware of the power of modern machine learning methods to infer even more sensitive information from very limited data. As users widely believe that not all data collected by the devices are actually necessary for their desired functionality, some participants in [37] reported to manually limit exposure to the device in certain situations by turning it off or avoiding entering its sensing range. Many participants mentioned to knowingly trade in privacy for comfort or utility of services, which might also be supported by a seemingly high trust in the data privacy handling of established brands [35].

Both research groups concluded that designers of smart home devices should try to improve the user interaction when it comes to explicit privacy settings but also that transparency

of both data collection and potential privacy implications of certain data should be an important design goal [35].

In [36], researchers investigated another privacy effect of smart speakers aside from data storage related aspects. They interviewed participants about their experience with sharing such devices. In this setup, data disclosure was not towards an unknown or abstract background entity but to people in direct interaction with the participant. When asked about sensitive data, users were referring to much more detailed aspects such as specific types of appointments in a calendar, data about specific routines or conversations with certain persons. Coping strategies were very similar to the previous studies in that people tried to avoid certain features (e.g., phone call) that recorded specific types of data, or they just accepted the risks to trade in for utility and the comfort of not needing to deal with the complex privacy-related user interfaces. However, some interviews also showed that disclosing potentially private information between group members could increase trust and closeness between them. If users have different expertise or roles (administrator) with the system, there is a potential for strong imbalances in perceived but also effective user privacy [38].

When examining the literature on smart systems, we can see that privacy discussions primarily focus on external privacy threats, how users perceive their privacy risks regarding hackers, industry or even governments and measures of how to address them. How users can govern personal data, which might be disclosed to other users ("Social privacy") within normal operation, is much less in the focus of the responses.

B. *Telepresence and Teleoperation*

Devices that are used to connect people over distance provide a natural and broadly established group of technologies that explicitly put the focus on privacy in communication involving multiple users. A general audio and video connection is part of the utility of such systems and the privacy implication will naturally need to be shifted to more detailed aspects. For example, a survey in [39] investigated what items users would like to hide from a remote controller. In their scenario an unknown individual from a cleaning company teleoperates a robot in the user's home. In this setting participants reported the highest sensitivities for items related to financial values. Similarly, Krupp and colleagues [40] presented interviews where they confronted participants with three telepresence scenarios that involved an unknown remote operator or a company supervisor. They again found the biggest concern for informational privacy around disclosing for example banking or health information to outsiders. These issues could be further categorized into security- versus embarrassment-related problems. Social/Interaction privacy aspects were rarely mentioned, most probably because of the settings that lacked specific interactions between the user and operator. The robotic device used for telepresence did not seem to play a big role in the reaction of the participants.

It can be stated that telepresence robots seem to mostly trigger privacy issues related to information security, similar to the results for smart devices. Specific privacy aspects about the interaction between the involved humans are mostly the same as in human-human interaction scenarios (e.g., embarrassment), but the existing studies did not show any specific impact of the robotic embodiment on such privacy aspect. However, the latter was usually also not in the focus of the research and the scenarios were not framed in a social context, where this could play a bigger role.

C. *Social Robots and Artificial Companions*

Social robots and artificial companions have been less researched from a privacy standpoint, especially based on empirically investigations [41](but see [44], [45]). Lutz at al. [41] discuss privacy in social robotics after conducting interviews with experts from both the robotics and the privacy area. We will briefly present two concerns from the discussion. One privacy issue relates to the presumption that users of embodied companions might more easily build intimate relationships with their device compared to screen devices or voice assistants. Within their social and emotional relationship, the robot might collect information which is more sensitive [41]. From a privacy design perspective, the need to protect the collected data as well as to implement mechanisms to inform users and give control become consequently more important. Furthermore, an intimate human-robot relation opens the possibility to be exploited.

Other concerns are discussed as psychological privacy effects. Lutz et al. refer to literature which discusses potential conformity effects and loss of freedom when a social robot is permanently present – in particular when the robot can operate freely in the home [41]. Psychological effects have already been observed in the IoT and smart speaker realm (as described before). However, there is no empirical evidence yet that conformity effects will increase when such devices appear as social entities.

In [42], researchers exposed a small number of participants to scenarios in which a social robot uses personal information about its owner in a discussion between the owner and a second person. All robot responses were designed to correct a statement of the owner, which is revealing true information that (s)he seemingly did not want to disclose directly. Participants were not completely comfortable with such a robot storing personal information at all but usually considered a trade-off with the robot's utility. One of the biggest concerns mentioned was storage of information about user personality. Luria et al. [43] created a large number of storyboards of a personal AI assistant interacting with a group of humans and discussed these with families with a focus on privacy and utility related aspects. The behaviors of the robot and their influence on human-human interaction could be classified in a number of categories, amongst them proactivity (interfering without an explicit request) or judgement. They also explicitly excluded data/information storage of privacy-related aspects and focused on the social implications. From the responses it was clear that there are many different aspects that need to be considered for a system behavior respecting people's privacy, such as the social relationship of the people in the audience (parent-child, outsiders-family, etc.) or the explicit utility of a certain information in a given situation.

IV. Discussion

When considering the results of previous studies, we must keep in mind that they are primarily investigating mental models of people about such devices. Owners of IoT devices

and smart speakers might even have done some privacy assessment before purchasing, with the result that their functional needs outperform the privacy risks. In contrast, telepresence and social robotics studies usually get their results from participants that have to imagine the functional implications of such devices, as very few had prior experience with an actual product. In many of these cases, it is difficult to separate hypothetical privacy implications from hypothetical utilities, given the tendency of participants in the reported research to provide feedback based on a trade-off between these two. We have also seen that most robotics-related research still focusses on data sharing/storage-related privacy, an area that likely shares many implications with prior research on more general data protection aspects. Interactions with more than one user affect the privacy implications and introduce more social aspects, which however are more complex in nature and also less understood based on the few existing empirical research studies.

Nevertheless, these studies are a good starting point to discuss about users' privacy needs for domestic robot mediators. Topics for which we believe that we could transfer previous insights to the mediation setting are:

- **Data Storage:** Local storages and data ownership seems to be appreciated by users of all smart home devices. As a robot can actively gather data and cover different areas of a location, what and when data is shared is even more implicit than in traditional approaches. We would argue that this should lead to an even higher responsibility of the designers to provide adequate means to protect such data or to implement user interfaces for privacy settings with a high transparency. Some information for the purpose of mediation might also have a specific temporal or contextual relevance. Installing mechanisms which set an expiry date to all data might be a measure to reduce privacy risks.
- **Surveillance:** Devices that collect video or audio data can also cause the feeling of being observed. People will likely not perceive robotic mediators differently in this regard, but embodied agents have the possibility to use active behaviors to counter such privacy implications, for example by turning away in certain moments. Some people adapt their usual behavior when feeling observed to avoid sharing certain information and a robotic device could have the potential to react to such a behavior with explicit privacy-enhancing behavior. An interesting direction of research could also be to investigate how a robot can influence perceived privacy in a group setting.
- **Transparency:** The lack of effective notice and control of data gathering and what information is stored is another issue that users frequently mention. Many participants in the cited studies also believe that devices are recording much more information than necessary. For smart devices and future robot mediators, situated feedback and control options like visual or auditory signals or a temporal "incognito mode" might help to improve user experience (e.g., [46]). How to inform users before actually sharing information is a different perspective, which however is much less researched. In the mediation context, this might be particularly challenging as sharing happens in a situation with other people present which might prevent using means that are publicly perceivable.
- **Accidental Disclosure:** Privacy implications of assistance systems used in group situations were mostly caused by accidental disclosure or insufficient authentication mechanisms. Information shared with one user could be heard or seen by bystanders or people could access calendars and reminders of other users. In existing devices dedicated user profiles or explicit access rights can partially prevent such situations but might only work in an all-or-nothing fashion. When disclosing towards other humans is part of the intended functionality, we do not need measures for security and general prevention, but rather mechanisms to decide in which context it is appropriate to use specific information and consider the effect of different forms of disclosure for a given piece of information. Defining different classes of recipients along a social dimension might be one direction to address. Robotic mediators will generally need more sophisticated understanding of interactions between multiple humans, but how this can support privacy enhancing data use is another open question.

Compared to IoTs and smart speakers, the focus of a privacy design might need to expand from input-privacy (what is recorded and stored where) to output privacy (how and in which context information can be disclosed). Equivalently, future research might have to include more aspects of social privacy. One of the implications would be to further investigate the possible difference in privacy evaluations when information is used in proactive behavior. Participants in [43] had mixed feelings about proactive activities, although it is hard to separate effects of controllability, transparency and utility based on their study design.

We reviewed research investigating the privacy implications from a user's perspective for related concepts such as smart speakers and social robots and showed that some of the findings could transfer to the social mediation setting. However, we also showed that there will be specific additional challenges that come with a focus on explicit sharing of acquired information during interactions between the original user and other people. Robot mediation in a domestic setting as has great potential to improve social relation and cooperation between humans. However, we would strongly argue for a privacy-aware design of any functionality or device, as this will become a key point for acceptance and trust of robots in a symbiotic society.

REFERENCES

[1] C. Breazeal, K. Dautenhahn, and T. Kanda, "Social robotics," in *Springer Handbook of Robotics*, B. Siciliano and O. Khatib, Eds. Springer, Cham, 2016, pp. 1935–1971.

[2] S. Sebo, B. Stoll, B. Scassellati, and M. F. Jung, "Robots in Groups and Teams: A Literature Review," *Proc. ACM Human-Computer Interact.*, vol. 4, no. CSCW2, pp. 1–36, Oct. 2020, doi: 10.1145/3415247.

[3] S. Shen, P. Slovak, and M. F. Jung, "'Stop. I See a Conflict Happening.': A Robot Mediator for Young Children's

Interpersonal Conflict Resolution," in *13th ACM/IEEE International Conference on Human-Robot Interaction (HRI 2018)*, Feb. 2018, pp. 69–77, doi: 10.1145/3171221.3171248.

[4] M. F. Jung, D. DiFranzo, B. Stoll, S. Shen, A. Lawrence, and H. Claure, "Robot Assisted Tower Construction - A Resource Distribution Task to Study Human-Robot Collaboration and Interaction with Groups of People," Dec. 2018. doi: 10.48550/arxiv.1812.09548.

[5] S. Gillet, M. T. Parreira, M. Vázquez, and I. Leite, "Learning Gaze Behaviors for Balancing Participation in Group Human-Robot Interactions," in *17th ACM/IEEE International Conference on Human-Robot Interaction (HRI 2022)*, 2022, pp. 256–274, doi: 10.5555/3523760.

[6] V. Charisi, L. Merino, M. Escobar, F. Caballero, R. Gomez, and E. Gómez, "The Effects of Robot Cognitive Reliability and Social Positioning on Child-Robot Team Dynamics," in *IEEE International Conference on Robotics and Automation (ICRA 2021)*, 2021, vol. 2021-May, pp. 9439–9445, doi: 10.1109/ICRA48506.2021.9560760.

[7] H. Brock, T. H. Weisswange, S. Thill, M. F. Jung, and A. J. Horowitz, "Exploring the Roles of Robots for Embodied Mediation," 2022, [Online]. Available: https://mypersonalrobots.org/events/2022/5/23/exploring-the-roles-of-robots-for-embodied-mediation.

[8] M. Rueben *et al.*, "Themes and Research Directions in Privacy-Sensitive Robotics," in *IEEE Workshop on Advanced Robotics and its Social Impacts (ARSO 2018)*, Jan. 2018, vol. 2018-Septe, pp. 77–84, doi: 10.1109/ARSO.2018.8625758.

[9] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*. European Parliament and Council of the European Union, 2016, pp. 1–88.

[10] *California Consumer Privacy Act of 2018*. California, USA: State of California Department of Justice, 2018, pp. 1798.100-1798.199.100.

[11] T. Heuer, I. Schiering, and R. Gerndt, "Privacy-centered design for social robots," *Interact. Stud.*, vol. 20, no. 3, pp. 509–529, Nov. 2019, doi: 10.1075/IS.18063.HEU/CITE/REFWORKS.

[12] M. Tonkin *et al.*, "Embodiment, Privacy and Social Robots: May I Remember You?," in *9th International Conference on Social Robotics (ICSR 2017)*, 2017, vol. 10652 LNAI, pp. 506–515, doi: 10.1007/978-3-319-70022-9_50/COVER.

[13] K. Caine, S. Ŝabanović, and M. Carter, "The effect of monitoring by cameras and robots on the privacy enhancing behaviors of older adults," in *7th ACM/IEEE International Conference on Human-Robot Interaction (HRI 2012)*, 2012, pp. 343–350, doi: 10.1145/2157689.2157807.

[14] S. Petronio, *Boundaries of Privacy - Dialectics of Disclosure*. State University of New York Press, 2002.

[15] A. Cavoukian, "Privacy by design: The 7 foundational principles," 2009. [Online]. Available: https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf.

[16] M. Dietrich, "Towards Privacy-preserving Personalized Social Robots By Enabling Dynamic Boundary Management," 2019, [Online]. Available: https://longtermpersonalizationhri.github.io/papers/PLOT-HRI19_paper_4.pdf.

[17] H. Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press, 2009.

[18] S. Thunberg, L. Rönnqvist, and T. Ziemke, "Do Robot Pets Decrease Agitation in Dementia Patients?," in *12th International Conference on Social Robotics (ICSR 2020)*, Nov. 2020, vol. 12483 LNAI, pp. 616–627, doi: 10.1007/978-3-030-62056-1_51.

[19] K. Wada, T. Shibata, T. Saito, and K. Tanie, "Effects of robot assisted activity to elderly people who stay at a health service facility for the aged," in *IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS 2003)*, 2003, vol. 3, pp. 2847–2852, doi: 10.1109/IROS.2003.1249302.

[20] H.-L. Cao *et al.*, "Robot-Enhanced Therapy: Development and Validation of Supervised Autonomous Robotic System for Autism Spectrum Disorders Therapy," *IEEE Robot. Autom. Mag.*, vol. 26, no. 2, pp. 49–58, Jun. 2019, doi: 10.1109/MRA.2019.2904121.

[21] S. Jeong *et al.*, "A Robotic Positive Psychology Coach to Improve College Students' Wellbeing," in *29th IEEE International Conference on Robot and Human Interactive Communication (RO-MAN 2020)*, Aug. 2020, pp. 187–194, doi: 10.1109/RO-MAN47096.2020.9223588.

[22] M. Chita-Tegmark and M. Scheutz, "Assistive Robots for the Social Management of Health: A Framework for Robot Design and Human–Robot Interaction Research," *Int. J. Soc. Robot.*, vol. 13, no. 2, pp. 197–217, Apr. 2021, doi: 10.1007/S12369-020-00634-Z/FIGURES/2.

[23] M. L. Traeger, S. Strohkorb Sebo, M. F. Jung, B. Scassellati, and N. A. Christakis, "Vulnerable robots positively shape human conversational dynamics in a human–robot team," *Proc. Natl. Acad. Sci.*, vol. 117, no. 12, pp. 6370–6375, Mar. 2020, doi: 10.1073/PNAS.1910402117.

[24] H. Erel, E. Carsenti, and O. Zuckerman, "A Carryover Effect in HRI: Beyond Direct Social Effects in Human-Robot Interaction," in *17th ACM/IEEE International Conference on Human-Robot Interaction (HRI 2022)*, 2022, pp. 342–352, doi: 10.5555/3523760.3523807.

[25] H. Tennent, S. Shen, and M. F. Jung, "Micbot: A Peripheral Robotic Object to Shape Conversational Dynamics and Team Performance," in *14th ACM/IEEE International Conference on Human-Robot Interaction (HRI 2019)*, Mar. 2019, pp. 133–142, doi: 10.1109/HRI.2019.8673013.

[26] N. Einecke and T. H. Weisswange, "Detecting Availability to Facilitate Social Communication," 2022.

[27] H. Brock, S. Sabanović, and R. Gomez, "Remote You, Haru and Me: Exploring Social Interaction in Telepresence Gaming With a Robotic Agent; Remote You, Haru and Me: Exploring Social Interaction in Telepresence Gaming With a Robotic Agent," 2021, Accessed: Jun. 07, 2021. [Online]. Available: https://doi.org/10.1145/3434074.3447177.

[28] L. Yang and C. Neustaedter, "Our House: Living Long Distance with a Telepresence Robot," *Proc. ACM Human-Computer Interact.*, vol. 2, no. CSCW, pp. 1–18, Nov. 2018, doi: 10.1145/3274459.

[29] K. Jeong *et al.*, "Fribo: A Social Networking Robot for Increasing Social Connectedness through Sharing Daily Home Activities from Living Noise Data," in *13th ACM/IEEE International Conference on Human-Robot Interaction (HRI 2018)*, 2018, pp. 114–122, doi: 10.1145/3171221.3171254.

[30] R. Albers *et al.*, "Meaningful Telerobots in Informal Care - A Conceptual Design Case," 2022.

[31] A. M. H. Abrams and A. M. Rosenthal-von der Pütten, "I–C–E Framework: Concepts for Group Dynamics Research in Human-Robot Interaction," *Int. J. Soc. Robot.*, vol. 12, no. 6, pp. 1213–1229, Dec. 2020, doi: 10.1007/s12369-020-00642-z.

[32] L. Tickle-Degnen, M. Scheutz, and R. C. Arkin, "Collaborative Robots in Rehabilitation for Social Self-Management of Health," Georgia Institute of Technology, Atlanta, GA, USA, 2014. Accessed: Aug. 19, 2022. [Online]. Available: https://smartech.gatech.edu/handle/1853/52674.

[33] P. Emami-Naeini, Y. Agarwal, L. Faith Cranor, and H. Hibshi, "Ask the experts: What should be on an IoT privacy and security label?," in *IEEE Symposium on Security and Privacy (SP 2020)*, May 2020, pp. 447–464, doi: 10.1109/SP40000.2020.00043.

[34] C. Lutz and G. Newlands, "Privacy and smart speakers: A multi-dimensional approach," *Inf. Soc.*, vol. 37, no. 3, pp. 147–162, 2021, doi: 10.1080/01972243.2021.1897914/SUPPL_FILE/UTIS_A_1897914_SM1205.DOCX.

[35] S. Zheng, N. Apthorpe, M. Chetty, and N. Feamster, "User perceptions of smart home IoT privacy," *Proc. ACM Human-Computer Interact.*, vol. 2, no. CSCW, p. 20, Nov. 2018, doi: 10.1145/3274469.

[36] Y. Huang, B. Obada-Obieh, and K. Beznosov, "Amazon vs. My Brother: How Users of Shared Smart Speakers Perceive and Cope with Privacy Risks," 2020, doi: 10.1145/3313831.

[37] M. Tabassum, T. Kosiński, and H. R. Lipford, "'I don't own the data': End User Perceptions of Smart Home Device Data Practices and Risks," in *15th Symposium on Usable Privacy and Security (SOUPS 2019)*, 2019, pp. 435–450, Accessed: Aug. 19, 2022.

[Online]. Available: https://www.usenix.org/conference/soups2019/presentation/alqhatani.

[38] E. Zeng, S. Mare, and F. Roesner, "End User Security and Privacy Concerns with Smart Homes," in *13th Symposium on Usable Privacy and Security (SOUPS 2017)*, 2017, pp. 65–80, Accessed: Aug. 15, 2022. [Online]. Available: https://www.usenix.org/conference/soups2017/technical-sessions/presentation/acar.

[39] S. Balali, R. T. Sowell, W. D. Smart, and C. M. Grimm, "Privacy Concerns in Robot Teleoperation: Does Personality Influence What Should Be Hidden?," in *11th International Conference on Social Robotics (ICSR 2019)*, 2019, vol. 11876 LNAI, pp. 719–729, doi: 10.1007/978-3-030-35888-4_67.

[40] M. M. Krupp, M. Rueben, C. M. Grimm, and W. D. Smart, "A focus group study of privacy concerns about telepresence robots," in *26th IEEE International Symposium on Robot and Human Interactive Communication (RO-MAN 2017)*, Dec. 2017, pp. 1451–1458, doi: 10.1109/ROMAN.2017.8172495.

[41] C. Lutz, M. Schöttler, and C. P. Hoffmann, "The privacy implications of social robots: Scoping review and expert interviews:," *Mob. Media Commun.*, vol. 7, no. 3, pp. 412–434, Sep. 2019, doi: 10.1177/2050157919843961.

[42] D. S. Syrdal, M. L. Walters, N. R. Otero, K. L. Koay, and K. Dautenhahn, "'He Knows When You Are Sleeping' — Privacy and The Personal Robot Companion," in *AAAI Workshop Human Implications of Human-Robot Interaction*, 2007, pp. 28–33, Accessed: Aug. 17, 2022. [Online]. Available: https://www.aaai.org/Library/Workshops/2007/ws07-07-006.php.

[43] M. Luria, R. Zheng, B. Huffman, S. Huang, J. Zimmerman, and J. Forlizzi, "Social Boundaries for Personal Agents in the Interpersonal Space of the Home," Apr. 2020, doi: 10.1145/3313831.3376311.

[44] C. Lutz and A. Tamó-Larrieux, "The Robot Privacy Paradox: Understanding How Privacy Concerns Shape Intentions to Use Social Robots," *Human-Machine Commun.*, vol. 1, pp. 87–111, 2020, doi: 10.3316/INFORMIT.097053479720281.

[45] M. Rueben, W. D. Smart, C. M. Grimm, and M. Cakmak, "Privacy-sensitive robotics," in *ACM/IEEE International Conference on Human-Robot Interaction (HRI 2017)*, Mar. 2017, pp. 425–426, doi: 10.1145/3029798.3029805.

[46] F. Schaub, R. Balebako, A. L. Durity, and L. F. Cranor, "A Design Space for Effective Privacy Notices," 2015.