Balancing personalization and privacy: datafication challenges in socially assistive robotics for older persons

Mannheim, I.; Edan, Y.; Peine, A.; Nimrod, G.

Routledge
Taylor & Francis Group

Information, Communication & Society

ISSN: 1369-118X (Print) 1468-4462 (Online) Journal homepage: www.tandfonline.com/journals/rics20

Balancing personalization and privacy: datafication challenges in socially assistive robotics for older persons

Ittay Mannheim, Yael Edan, Alexander Peine & Galit Nimrod

To cite this article: Ittay Mannheim, Yael Edan, Alexander Peine & Galit Nimrod (23 Jun 2026): Balancing personalization and privacy: datafication challenges in socially assistive robotics for older persons, Information, Communication & Society, DOI: 10.1080/1369118X.2026.2693162

To link to this article: https://doi.org/10.1080/1369118X.2026.2693162

Published online: 23 Jun 2026.

INFORMATION, COMMUNICATION & SOCIETY
https://doi.org/10.1080/1369118X.2026.2693162

Balancing personalization and privacy: datafication challenges in socially assistive robotics for older persons

Ittay Mannheim [a,b], Yael Edan [c], Alexander Peine [d] and Galit Nimrod [a]

[a]Department of Communication Studies, The Center for Multidisciplinary Research in Aging, Ben-Gurion University of the Negev, Be'er Sheva, Israel; [b]Department of Methodology and Statistics, Institute of Psychology, Leiden University, Leiden, The Netherlands; [c]Department of Industrial Engineering and Management, ABC Robotics Initiative, Ben-Gurion University of the Negev, Beer-Sheva, Israel; [d]Department of Digital Culture, Innovation and Communication, Open University of theNetherlands, Heerlen, the Netherlands

ABSTRACT

The promise of Socially Assistive Robots (SARs) to deliver personalized care for older persons depends heavily on extensive data collection, raising concerns about privacy, autonomy, trust, and the limited involvement of older adults in shaping data-related configurations. This study examines how developers and researchers navigate the tension between personalization and privacy in the datafication process in SAR development for older people. We conducted eighteen interviews with international experts from industry and research institutes and analyzed them using a constructivist grounded theory approach. Participants identified 41 unique data types used by SARs, comprising numerous variables. In describing the datafication of older persons as SARs users, participants characterized SARs as capable of 'collecting everything.' Regulatory compliance and data safeguarding were framed in 'all or nothing' terms, leaving older adults uninvolved in personalizing or influencing data management and control over their data, effectively requiring them to accept the SAR as a whole or decline it entirely. At the same time, participants viewed control, transparency, personalization, and the storage of personal data for user identification as essential for effective social robotics. These findings reveal a personalization-data-storing paradox: privacy preserving practices and regulatory constraints often restrict data use and online connectivity, yet meaningful personalization and interaction depend on richer data use and access. We illustrate this paradox through a typology of four SAR categories and highlight the need to involve older persons in shaping meaningful data management practices that balance privacy protection with an enriched user experience.

ARTICLE HISTORY
Received 23 November 2025
Accepted 17 June 2026

KEYWORDS
Ageism; older persons; datafication; personalization; privacy; socially assistive robots

CONTACT Ittay Mannheim ittay.mannheim@gmail.com POB653, Beer-Sheva 8410501, Israel

1. Introduction

Socially assistive robots (SARs) are increasingly viewed by developers and policymakers as a potential solution to support the care needs of older adults while alleviating financial pressure of health and care systems (Maibaum et al., 2022). Despite facing technological, ethical, and economic challenges, SARs are developed to provide physical, cognitive, emotional, and social support, with the intention of helping older adults maintain autonomy, enhance well-being, and postpone reliance on formal care services (Kearney et al., 2018; Maibaum et al., 2022; Zafrani & Nimrod, 2019). Realizing this potential, however, depends on collecting and processing large volumes and diverse types of data, including personal data. The quantification and storage of social and behavioral data used to predict and support meaningful interactions is often referred to as 'datafication' (Ruckenstein & Schüll, 2017). While such data enables personalized and adaptive interactions with SARs, it also raises concerns and risks related to privacy, autonomy, trust, and the extent to which older users are involved in shaping their data-related configurations. Developing meaningful and personalized experiences, while safeguarding user privacy, are thus often perceived as contradicting goals and expose an inherent tension that must be carefully balanced.

This study examines how developers and researchers consider and address this tension within the datafication process when developing SARs for older adults.

SARs typically require a broad spectrum of data, seen as a prerequisite for establishing meaningful interactions. SARs rely on cameras and embedded sensors (Chuah et al., 2021), often integrated with wearables, smart devices, and information systems to monitor and assist older persons and their caregivers in daily activities (Kearney et al., 2018). Machine learning algorithms process location and sensory inputs from cameras, microphones, and motion detectors enabling robots to perceive and respond to the environment (Clark et al., 2019). Biometric data (e.g., facial recognition and voice analysis) support user identification and personalization (Fosch-Villaronga & Mahler, 2021). Additionally, contextual and behavioral data, including user preferences, routines, social networks, and health metrics, enable SARs to recognize social relationships and interactions (Grabler & Koeszegi, 2025), detect emotional states (Dietrich et al., 2023), and anticipate user needs to facilitate appropriate companionship and support (Gallistl & Von Laufenberg, 2024). To maintain continuity, coherence, and create a sense of trust of the user in the SARs capabilities, at least part of this data must be stored, so the robot can 'remember' past interactions (Clark et al., 2019).

While previous studies have emphasized the challenges of collecting large amount of personal data and highlighted the importance of involving older persons in the development of SARs (Gasteiger et al., 2022; Mannheim et al., 2025), none have specifically examined this involvement regarding datafication and how developers and researchers perceive these challenges and handle them in practice. This study addresses this gap by investigating how these stakeholders perceive and navigate the tension of data collection needed for personalization while maintaining privacy and avoiding harm. As well as how they consider the role of older persons in shaping datafication processes within SAR development. Particularly, we investigate: (1) What data SARs use and require for fulfilling their purpose as personalized assistive devices, (2) what reactions and concerns designers and researchers encounter from intended users regarding such data, and how they navigate them, and (3) how are older adults involved in the development process of data collection and management practices, and how this shapes the datafication of older persons in SARs.

2. Related research

Older adults are a key target group for SARs, particularly as populations age and caregiving resources become constrained (Neven, 2010). Adoption, however, depends not only on functional benefits but on how well SARs align with users' diverse needs, contexts (cultural, physical, and social environments) and expectations. Interactions with SARs should be viewed therefore holistically, considering the heterogeneity of older adults (Zafrani & Nimrod, 2019). At the same time, SARs rely on extensive data collection and algorithmic processing, introducing potential harms and risks related to access (e.g., privacy breaches, bias or misuse of personal data). Consequently, the notion of safeguarding privacy has become anything but straightforward, leading to clashes around asymmetries of control between older adults and family members, caregivers, and institutions (Berridge & Wetle, 2020; Dalmer et al., 2022). As a result, key factors such as trust, perceived control, and personalization become tightly intertwined: while data-driven personalization can enhance usability and engagement, it may also reduce users' sense of control and undermine trust if data practices are opaque or intrusive. Accordingly, the adoption of SARs hinges on balancing the benefits of personalized assistance with transparent, user-centered approaches to data use that preserve autonomy, privacy and foster trust.

2.1. Access and risk of algorithmic harms

The extensive, and perhaps intrusive, datafication processes required for SARs introduce significant risks for 'algorithmic harms' (Diberardino et al., 2024; Shelby et al., 2023). Such harms include security risks in the form of breaches, unauthorized access, or misuse of health and biometric data (Fosch-Villaronga & Mahler, 2021) and the potential for identity theft. But potential harms extend beyond questions of data security because they involve the collection of sensitive information from potentially vulnerable users in personal spaces or via telepresence (Lutz & Tamó-Larrieux, 2020). This data collection is often opaque, as understanding of what is collected and how it is used requires technical understanding and continuous engagement. Although it is widely recognized that surplus behavioral data can be commercially exploited without the user's full awareness or informed consent (Zhu & Zhang, 2025), privacy risks also rise in non-commercial contexts. Even access by family members can violate the older adult's privacy, liberty, and dignity (Sharkey & Sharkey, 2012).

Furthermore, institutional access to data (by robot manufacturers and third-party providers) is particularly problematic because users might view robots as friends or companions and entrust them with personal, potentially sensitive information (e.g., passwords, personal information). Also, robots with advanced sensors can collect sophisticated data without the users' awareness, consent, or full comprehension of its extent (Lutz & Tamó-Larrieux, 2020). Such capacities can cause significant concerns among users regarding the trustworthiness of SARs in maintaining their privacy. For example, Krupp et al. (2017) reported privacy concerns of users about recording 'awkward moments' when interacting with telepresence robots. Xu et al. (2025) found that users were worried about potential misuse of data gathered during their interactions with robots without consent. Consequently, the continuous observation by 'data-hungry technologies' (Gallistl & Von Laufenberg, 2024) may alter natural behavior, discourage private activities, or reduce technology use altogether (Neven, 2010).

An important framework for examining the datafication of SARs for older persons is that of 'Algorithmic harms' portrayed by Shelby et al. (2023) in a taxonomy of socio-technical harms consisting: representational (e.g., stereotyping), allocative (opportunity or economic loss), quality-of-service (performance disparities across user groups), interpersonal (loss of agency or privacy violation), and societal harms. This research highlights how design decisions, norms, and power relations embed these harms. Nevertheless, while gender, race, or sexual orientation biases are discussed extensively, age-related bias is rarely addressed.

To reduce algorithmic harms, legislative frameworks aim to ensure ethical guidelines to promote safety and equality when using data and algorithms. For example, the European Commission's guidelines (2019) for trustworthy AI emphasizes several principles: (1) Human agency and oversight – AI should empower people and support informed decisions, (2) Technical robustness and safety, (3) Privacy and data governance – ensuring mechanisms to respect privacy and data protection and ensuring legitimized access to data, (4) Transparency – the data, system, and AI business models should be transparent and the way in which systems make decisions should be explainable to the users who must be informed of the system's capabilities and limitations, (5) Diversity, non-discrimination, and fairness – bias must be avoided, and all stakeholders should be engaged throughout the system lifecycle, (6) Societal and environmental well-being – AI should benefit society broadly, considering social and environmental impact, (7) Accountability – Mechanisms should ensure responsibility and accountability for AI systems and outcomes. Although such high-level principles can provide some guidance, they have not been translated into actionable rules for increasing trustworthiness and responsible implementation and customization of AI systems such as SARs (Lukkien et al., 2025).

2.2. Trust, control, and personalization

Trust in the functionality, usability, and safety of the interaction with SARs is crucial for their acceptance by older adults (Zafrani et al., 2023). Whereas privacy concerns, especially in complex settings such as healthcare, can surmount attitudes toward the robot's design (Jayaraman et al., 2024). Factors that influence trust include transparency in data collection and user control over privacy settings (Dietrich et al., 2023). Uncertainty about data handling or compromising privacy can reduce engagement (Grabler & Koeszegi, 2025). Furthermore, algorithmic biases in data represent an additional risk in robotic interactions. Emotional recognition and behavioral analysis algorithms trained on age-biased datasets (Rosales & Fernández-Ardèvol, 2019) may produce inappropriate responses of the robot and consequently reduce the trustworthiness of the interaction with it (Dietrich et al., 2023). Ensuring transparency and providing users with clear control over data can help mitigate these concerns and support ethical deployment (Grabler & Koeszegi, 2025). However, the meaning of transparency and what constitutes control in practice, remains unclear (van Leersum & Peine, 2025).

To foster trust and encourage acceptance, developers must implement stringent data protection and clear consent mechanisms that allow users to make informed privacy decisions (Sharkey & Sharkey, 2012). Customizable privacy settings and educational initiatives to enhance digital literacy can further increase users' sense of control and confidence in robots (Dietrich et al., 2023). However, the current design and implementation of such controls in SARs remain underexamined (Jayaraman et al., 2024). Ethical practices, including communication of understandable and transparent consent to data policies and robust security (Zhu & Zhang, 2025), are essential to ensure SARs are beneficial, non-intrusive, and support older adults' dignity. Currently, however, such communication is often mediated by external collaborators (e.g., technical support, caregivers) rather than integrated into the robot's design (Schött et al., 2023).

The potential of SARs to deliver personalized experiences is vital for their usefulness and acceptance by older persons, making their active involvement in the design process essential (Gasteiger et al., 2022). Nevertheless, SARs are often designed based on developers' assumptions, with limited consideration of older persons' actual needs or the perspective of their broader care networks (Søraa et al., 2023). This gap limits the development of meaningful communication about data management and the alignment of SARs functions with users' real preferences and expectations. Indeed, a key barrier to SARs implementation is 'technological determinism,' where developers assume a prescribed use, while users may have different expectations or use the technology in unforeseen ways (Peine & Neven, 2021).

In summary, a clear tension emerges between the need for extensive data to fulfill the promise of adaptable, personalized SARs and the imperative to safeguard privacy while ensuring transparency and user control over privacy. So far, the literature has not developed a clear understanding of how this tension is handeled in practice, and how the involvement of older adults shapes such practical handling.

3. Method

3.1. Design

This study is based on in-depth interviews with researchers and designers involved in co-designing SARs for older persons focusing on datafication processes taking place in the development of SARs. The interviews explored views on data-related aspects of SARs and how older persons were engaged in research and design processes concerning data collection and use.

3.2. Participants

A sampling matrix guided a purposive sampling designed to ensure a comprehensive and international perspective on SAR design. The matrix balanced gender, geographic location, and professional roles, distinguishing between researchers and developers (designers, entrepreneurs, and managers) engaged in SAR design projects for older persons.

Recruitment began with mapping the authors' professional networks, outreach to key figures identified through robotics conferences and industry, and snowball sampling of recommended contacts given by the participants. Participants received an information letter and consent form by email outlining the study objectives, interview duration, and relevant ethical considerations. Non-respondents received up to two follow-up reminders. Of 28 invited individuals, two declined participation, and eight did not respond or were unavailable. Ultimately, 18 participants were interviewed.

The sample was diverse in terms of age, education, professional experience, and involvement in research and design of a broad range of SAR types. The mean age was 40.9 years (SD = 11.1) and almost half (8/18) were women. Professional roles were evenly distributed between academic researchers (affiliated with universities or research institutions) and industry professionals (employed by private or public robotics companies or technology firms, including CEOs, directors, and product managers). Six industry participants also held research positions within their organizations.

Most participants (15/18) had technical backgrounds in engineering, computer science, AI, or physics. Two participants had expertise in the arts or film studies, while one possessed training as an occupational therapist. Many participants had pursued additional interdisciplinary training in fields such as cognitive science, psychology, user experience design, or conversational design. The sample reflected global representation (ranging from Europe, North America, the Middle East, Africa, Asia & Oceania). Seven participants conducted robotics work across multiple countries.

3.3. Tools and procedure

Interviews were conducted online ($n = 14$) or in person ($n = 4$) with one session involving two participants from the same organization. Sessions lasted 30–79 min (M = 49, SD = 13).

Informed consent was obtained before each interview, and study objectives were reiterated at the beginning of the interview. A semi-structured interview protocol guided the conversations. The interviews began with background questions exploring participants' entry into SAR research and design for older persons, their perspectives on using SARs, and experiences of involving older persons in development. Subsequent questions focused on datafication, addressing types of data required and collected by SARs, older persons' involvement or reactions to data practices, concerns raised and responses to them, and whether user involvement in design processes influenced datafication approaches.

Ethical approval was obtained from the first author's institutional review board (approval number 18052023a).

3.4. Analysis

Recognizing that researchers' and designers' perspectives on datafication in SAR may differ by backgrounds, experience with older persons, professional networks, and institutional context (academic versus commercial settings), we adopted a constructivist grounded theory approach (Charmaz, 2006). This approach facilitated a data-driven examination of the participants' experiences and perspectives.

Interviews were transcribed verbatim using Otter.ai software (https://otter.ai/) and manually reviewed against audio recordings, with key quotations documented. Transcripts were then returned to participants for validation and optional comments. The primary author conducted open and in vivo coding in Atlas.ti V.23. To enhance credibility and reliability, four transcripts were independently coded by a research assistant, with results discussed and reconciled. Two additional team discussions examined selected quotations and validated coding decisions.

The initial open coding phase yielded 89 codes (see Appendix for the full division of themes, categories, and codes). Saturation was reached after 18 interviews, as fewer new codes appeared in later interviews. Special attention was paid to explicit and indirect references to data types collected and utilized by SARs as described by participants.

Codes were then consolidated and organized into broader categories through axial coding. Multiple iterative discussions within the research team refined and validated these categories, resulting in 20 final categories. These were subsequently grouped into three overarching themes described in the Results section.

To ensure anonymity, participants were assigned numbers used in quotations alongside gender and professional role (excluding age and nationality), thus providing context while preserving confidentiality. Quotations are preserved verbatim, and reporting follows the *Reframing Aging* guidelines to avoid ageist and implicit biases (GSA, 2023).

4. Results

4.1. 'The robot collected everything:' datafication in SARs for older persons

Throughout the interviews, participants specified 41 types of data collected and used by SARs, either for core functionality or during development and testing (see Table 1). Data types were grouped into nine categories. Most data types (65.6%) concerned user identification and engagement with the SAR, such as language use, emotional tone, positioning, monitoring and acceptance. The most frequently mentioned data types were video recording ($n = 10$), acceptance/rejection of use ($n = 10$), facial recognition ($n = 9$), social and personal information ($n = 8$), and trust ($n = 6$). Other data types corresponded with the most prominent SAR use cases for older persons, particularly healthcare and social-emotional support (Gallistl & Von Laufenberg, 2024; Mannheim et al., 2025). Participants also distinguished between data collected for research, learning, and development processes, and that required for real-time functioning.

Nonetheless, this descriptive account of the data types collected is based solely on participants' responses. The actual volume of data collected is likely much larger. Furthermore, each data 'type' may encompass multiple variables. For example, the data type 'health variables' encompass blood pressure, weight, and medications, which could be further categorized by temporal aspects (e.g., daily trends) or thresholds (e.g., low, high). Similarly, 'emotion classification' might include facial features (e.g., mouth, eyes, nose) alongside voice features such as pitch or valence. Even a data type like 'family time' could include day, time, duration, family members present, interaction type, and activities. Thus, the strands of data, including all related variables, involved in datafying older users may number in the hundreds.

Table 1. Data types mentioned by participants grouped by categories and organized by mentioning frequency.

Data category	Data types	Mentioning	Total mentioning	% mentioning
Digital engagement & interaction	Active engagement (frequency)	3	21	16.0%
	Interactions	6		
	Usage data	5		
	Robot task efficiency	1		
	User task success	1		
	Time of use	1		
	Safety	1		
	Interface	1		
	Reminders	2		
Acceptance	Satisfaction	1	20	15.3%
	Pleasurable	1		
	Willingness to use	2		
	Trust	6		
	Acceptance/rejection	10		
Face recognition & visual	Facial expression or recognition	9	20	15.3%
	Visual/ video recording	10		
	Eye contact with the robot	1		
Positioning monitoring and movement	Distancing	4	17	13.0%
	Gait/kinematic	2		
	Mapping	3		
	Monitoring	5		
	Movement (not video)	2		
	Position	1		
Social network & emotional	Family time	2	14	10.7%
	Social and personal information shared	8		
	Contacts	1		
	Emotions	3		
Research	Qualitative interview	4	13	9.9%
	Qualitative observational	4		
	Questionnaires	5		
Health	Hand grip/pressure	1	12	9.2%
	Impairment	1		
	Sleep	2		
	Health variables	5		
	Eating	2		
	Wearables recording physiological data	1		
Language, communication & audio	Choice of words, language, text	3	8	6.1%
	Sound/voice	4		
	Questions about the robot	1		
Activities & Gamification	Frequency of functionalities/ experiences	5	6	4.6%
	Level achieved (cognitive game)	1		

> In the nursing homes, you have family that come and visit, right? So, we're trying to capture data from that set of interactions, usually during the weekends, when the family will come visit their elderly … We tried to observe some of the activities, particularly when we receive the elderly getting excited and introducing that technology, the robots, to the family members, and they start to talk about it together (#105, man, researcher in a research institution).

All but one participant explicitly mentioned between 2 and 15 distinct data types ($M = 6.1$, $SD = 4.4$). The participant who mentioned the most data types emphasized that robots require vast data to assess engagement and could, in principle, collect 'everything:'

> She [the robot] collected a lot of data. First of all, everything you said to her was saved and recorded, and all the interaction plus metadata, like the time it was said or the whole intent … it doesn't matter … The whole conversation was saved. And when the robot asked certain things, then the values of your answers, like your name, where you grew up, your weight, if she [the robot] measures things like that on a daily or weekly or monthly basis. Also, if the whole point of this feature is to measure these things over time, she saves it. Everything. The contacts, you can save contacting. My son, what's his name, phone number, where he lives. And with the conversations, she would ask, 'How did you sleep?' So, she would save your sleep status over time. 'What did you eat today?' So, everything, everything, everything is saved (#103, man, product manager).

4.2. Legal frameworks – 'all or nothing'

Although legal compliance was not explicitly mentioned, many participants began by discussing regulatory adherence and privacy measures they implement when asked about SAR data types. In several cases, responses appeared somewhat defensive, with developers emphasizing the involvement of legal counsel and related costs, while researchers emphasized ethical approval and detailed consent procedures.

One participant, who did not identify any data types, even when explicitly prompted, repeatedly and carefully emphasized that no data is collected without consent:

> The data the robots collect is done with quality and informed consent. It's only collected locally. We also don't store the data between sessions unless it's stored locally, with informed consent. And this is so that it will be HIPAA [Health Insurance Portability and Accountability] compliant, GDPR [General Data Protection Regulation] compliant, COPPA [Children's Online Privacy Protection Act] compliant. Until all the robots are deployed with these safeguards, and that wouldn't prevent, say, one of the people who perhaps may buy the robot or use the robot to violate those … and you know, strip out our control system, but the way that we set up our software, it's done with data privacy, and security, that is hyper compliant with all the different privacy and security regulations (#116, man, CEO and designer).

As this quote exemplifies, compliance with privacy regulations, often driven by concerns about potential data breaches, led to precautionary data management practices among SARs developers and researchers. Though, as noted, commercial parties involved may eventually use SARs in less precautious and predicted ways. Several participants specifically mentioned the importance of deleting data between sessions, avoiding the collection of 'personal information,' and storing data only locally, on secure, offline systems or company/university computers. Additionally, several users noted that they deliberately avoid using video data collected by the robot itself due to privacy and ethics concerns:

> My robot itself didn't gather any data, didn't collect anything. So, any data that I wanted gathered, I recorded in different ways … I think it should be really transparent what's being recorded and why. And because of this whole ethical thing, that was like the big topic for me, I decided to not let the robot record anything and make sure that everything was very clear for the people what was being recorded. So, they could see the camera [behind the robot] the whole time, they could feel the wearable that they were wearing. And of course, they filled in the questionnaires themselves. So, they were very much aware of what was being recorded and why (#104, woman, researcher).

Later in the interview, the same participant broadened the discussion to AI in general, criticizing developers who 'either don't know or don't care about the consequences and just want to develop the thing they want to develop.' Other participants noted that regulatory frameworks differ across countries, and the design of SARs' data infrastructures, and AI systems more broadly, is shaped by geographical and cultural contexts. Nevertheless, some admitted that SARs must, in fact, collect personal information to enable functionality and personalized interactions, particularly when creating user IDs or profiles that enable the robot to recognize individuals in future interactions. Often, such information is provided by members of the user's social network:

> You must identify the person that the robot interacts with and connect it to a user profile that contains information that either comes from the caregivers, caretaker, or from the robot's previous interactions. And then you have to keep this data like we do when we interact with people, right? We treat different people differently (#128, man, researcher).

In this context, several participants highlighted a key limitation: Data collection in SARs is often perceived as 'all or nothing.' Users must either consent to the robot's full functionality and data collection policy or forgo using it altogether:

> Of course, people would not agree to a certain amount of information that we wanted to collect. We understood that and like OK, that's fine. So, you weren't, you know, a good candidate for this product (#102, woman, researcher and product manager in a private company).

Some participants (as in the latter example) justified the construction of such 'all or nothing' consent procedures because 'generally speaking, it didn't affect the design because what we learned is actually that just like most of the products we use, we don't really care about the data that's collected about us. We care about the benefit that we're able to get from the products that we use' (#102).

4.3. Perceptions of data usage, concerns, and personalization

In a previous study (Mannheim et al., 2025), we reported how participants emphasized that involving older persons in the design process is non-negotiable and imperative for designing effective good human-robot interaction. However, when discussing data and privacy, older adults seemed to be entirely uninvolved in the design of SARs' data infrastructures, procedures, and usage. While this was generally the case, participants often shared their own perceptions on data privacy, controllability, and personalization.

Building upon the previous examples, we now highlight the tension between privacy protection and usage optimization. On the one hand, privacy safeguards often lead to 'all or nothing' environments, limiting personalization, and excluding potential users who might disagree with lenient privacy policies. On the other hand, participants emphasized the users' need for more control, transparency, and personalization, which typically requires personal data and user identification.

> You can cover the cameras. And that's everyone. When I had [name of the robot] at home, then there was really even a piece of plastic that we made internally [in the company], to cover the camera. It's not like we marketed [the robot] with it, but there were people covering the cameras. But no, apart from that, there is no toggle programmed in the product, or options to activate certain things. It's either all or nothing … also, you know, these thoughts, it's not like we've ever really processed them … I mean, if you bring a robot with cameras and a speaker into the house, you probably care less about privacy. And if you care about privacy, it doesn't matter how many 'toggling' we implement (103, male, product manager).

Discussing his own experiences, this participant described practices such as covering the camera when testing the robot in his own home. However, when referring to other (older) users, privacy needs were dismissed based on the (perhaps stereotypical) assumption that older persons who agree to have a robot in their home do not care about privacy. This assumption, linking vulnerability with indifference to privacy, was also highlighted by other participants. It signifies yet another paradox: While older persons are considered as ideal SAR users due to factors like loneliness or the need for assistance, they are simultaneously deemed as unconcerned with privacy, despite well-documented evidence that trust and control over privacy are key barriers for SARs acceptance (Dietrich et al., 2023).

Participants also discussed concerns related to monitoring and surveillance. The mere presence of a camera, or even 'blinking eyes on a screen' can give the impression of constant observation ('the robot is always listening or watching'). Challenges included 'communicating to users what we are doing [with the robots, camera, and sensors] and what we are doing with the data' (#126, man, director and researcher in a private company). Participants emphasized that users need reassurance that their private data is protected, which led some participants to question online connectivity of the robot and the inherent tension between creating a social robot and collecting personal data to enable user recognition:

> The robot does require some data that would be considered highly sensitive, and the most obvious one is facial recognition. A robot that does not run facial recognition cannot be a social robot … So, people who say that they are not doing facial recognition on robots, they are lying, or they are not doing social robots. It's a requirement (#126, man, director and researcher in a private company).

Later on, this participant explained his concern with dealing with personal data:

> We are really trying hard not to store any private data on the robot because we don't want to get into the issues of having to manage them. Not being entirely offline helps. So, the speech recognition is done on the robot, the face recognition is done on the robot. If someone buys our robot and wants to connect it to the internet, then they can, but that comes with the responsibility of managing the data that they will store. But as a company selling robots, the robots are designed to operate entirely offline.

Safeguarding privacy is undoubtedly an important issue, and legislation exists for good reasons. SARs are often perceived as unsafe due to fear of surveillance and negative fictional and media representations (e.g., portraying SARs as agentic and dominating mankind). Nevertheless, effective privacy and data management can enhance trustworthiness. Complicated consent forms (e.g., Zhu & Zhang, 2025) and 'all or nothing' privacy settings most likely do not increase transparency or trustworthiness. Some participants described how certain fears 'were just a misunderstanding of what robots will work for, what robots are actually doing, and how helpful they could be' (124, woman, researcher). Other participants gave examples of how personalization of data infrastructures can contribute to safeguarding privacy while giving more control to the users, for example, by implementing a 'clear privacy button', creating personalized 'start key words', or clearly explaining the potential benefit of storing certain data (e.g., being able to send data to your personal doctor in real time). As with other aspects of SAR design, participatory approaches were emphasized as beneficial in addressing and personalizing data and privacy issues:

> But I also think that's [privacy] one of the key points in participatory design … This elderly group that came the other day … they were at first, 'No, no, no, my data shouldn't be … nothing is sent outside,' … But then just by talking about the pros and cons of doing that … and in this case of my health, then my GP wants to know that I'm going through these things. So, if they understand that they are the ones saying 'no,' actually, it's okay, as long as I can say which data goes to whom. And that was the key for them (#127, woman, researcher in a private company).

5. Discussion

Synthesizing the three themes revealed several tensions converging into a main paradox in SARs datafication design – the 'personalization-data-storing' paradox. Participants highlighted two key tensions: (1) whether SARs use and store personal data to enable future interactions? (2) whether connecting robots online compromises data integrity and security?

This paradox reflects a fundamental trade-off: avoiding storage of personal data supports privacy protection and regulatory compliance, but also constrains the SAR's ability to deliver meaningful personalized interactions.

Using a two-by-two matrix, we map the tradeoffs between tensions and ethical dilemmas to propose a theoretical typology of four SAR categories. Illustrated in Figure 1, the typology highlights a third tension: between safeguarding privacy through rigid 'all or nothing' settings and consent procedures, and addressing users' needs for greater control, transparency, and personalized experiences. The bottom-left quadrant represents a SAR that neither stores personal data nor connects online. This robot seems to be compliant

Using / storing personal data or preferences	Limited personalization. Usable in limited contexts. Concern for privacy related to access to the SAR.	High potential for personalization. High concern for privacy. Concern of surveillance and consent.
Not using / erasing personal data or preferences	No personalization outside a single session – the robot does not remember the user. Limited capabilities. Low risk for privacy.	Practical (information, tasks), playful, useful for limited interactions. Risk for privacy dependent on the type of online interactions.
	Robot offline	**Robot online**

Figure 1. Typology of four SARs demonstrating the 'personalization-data-storing' paradox.

with regulations, but may be very limited in functionality, unable to recognize the user or provide social or personalized interactions outside of a single session. The SAR in the top-left quadrant stores personal data off-line, allowing local personalization within controlled predefined environments (e.g., a lab). Concern for privacy is related to the question of who has access to the SAR (and the data), and which agreements were made with the user. The bottom-right quadrant presents a SAR that connects online, but does not store personal information, enabling more interactive options, or playful personalized interactions, yet still limited to single sessions. Risk for privacy is lower with this SAR but may increase depending on the type of interactions performed online, and the types of data required for those interactions. Lastly, the SAR on the top-right quadrant both stores personal data or preferences and connects online, potentially offering recognition, continuous personalization and multi-environment use, but may also raise significant privacy, legal, and ethical concerns, which should be addressed and clarified for the user. Importantly, the typology does not necessarily reflect specific available robots, as settings, hardware, and software can be added and modified by manufacturers or users. Rather, it reflects (often arbitrary) choices made by researchers, designers, and users that simultaneously affect datafication and personalization.

Several paradoxes related to the personalization-data-storing paradox have been previously discussed in the literature. The 'privacy paradox' (Kokolakis, 2017) describes how users, despite expressing privacy concerns, tend to consent to sharing personal data in order to use services or products. Explanations suggest this reflects power imbalances, or even 'dark patterns' (Waldman, 2020), where meaningful choices are limited and users prioritize benefits over the burden of understanding privacy policies. This can also be understood in terms of the trade-off between benefiting from using the product and agreeing to the privacy terms, despite feeling less control (Slane & Pedersen, 2025). Similarly, the 'robot-privacy paradox' shows that perceived benefits of social robots override privacy concerns (Lutz & Tamó-Larrieux, 2020), with users primarily worried about data protection of the manufacturer, followed by social and physical concerns. A particular power imbalance currently embedded in SARs designs for older persons corresponds with the involvement of others in the person's social and care network, often providing private information, overriding the older adults' autonomy and control (Berridge & Wetle, 2020; Dalmer et al., 2022; Sharkey & Sharkey, 2012).

In our study, participants mainly treated privacy as a compliance issue, resulting in 'all or nothing' approaches. Notably, frameworks such as the GDPR primarily define the obligations of data collectors toward the state rather than toward citizens or users, and do not necessarily involve ethical considerations. While older people might initially accept SARs, issues of trust and control over privacy remain key barriers for long-term adoption (Dietrich et al., 2023), yet are under-researched compared with other acceptance factors (Felding et al., 2023). Moreover, Coghlan et al. (2021) found that SARs designed to enhance independence could paradoxically increase feelings of dependency when users experience low perceived control or reduced dignity (Zhang et al., 2024). Brandimarte et al. (2013) emphasized a 'control-paradox,' where increased (perceived) control over privacy led participants to higher disclosure of personal information, thus potentially increasing their risk for exposure.

Greater transparency about data use and insights can enhance users sense of autonomy (Søraa et al., 2023). Importantly, more transparency should not be confused with merely adjusting consent to privacy policies. Grabler and Koeszegi (2025) suggest a holistic, multi-dimensional approach to privacy including five strategies: privacy by design, transparency, control, regulation, and contextual integrity. Our findings suggest that, rather than relying on rigid 'all of nothing' privacy by design approaches, data and privacy configurations should incorporate user control, be explainable and transparent, and remain adaptable overtime to changing social networks or personal preferences (Søraa et al., 2023). Personalization in privacy and data infrastructures as such should follow the understanding that 'one size does not fit all' (Coghlan et al., 2021), which can help overcome a key barrier to SAR implementation.

While transparency is often seen as a way to boost trust in AI-driven technologies (Weitz et al., 2019), improving transparency and providing explanations does not always lead to positive evaluations (Ananny & Crawford, 2018). Explaining multiple AI technologies in social robots can confuse users, raise privacy concerns, and weaken trust (De Graaf et al., 2021). Xu et al. (2025) found that explainable AI can reduce privacy concerns and increase acceptance but has its limits: Combining transparency for both speech and facial recognition increased privacy concerns and elicited negative feelings compared to disclosing facial recognition alone. The examples above, together with our findings, highlight the value of participatory approaches in designing SAR data practices with and for older persons (Gasteiger et al., 2022; Søraa et al., 2023). Such approaches can support the development of clearer, explainable, and personalized data and privacy management. Future research could inquire if this in turn may enhance a sense of control and transparency, while providing safety and supporting SARs' intended roles and imagined use-cases.

Revisiting the European Commission's guidelines (2019) for trustworthy AI, this study offers insights into their practical implementation in SAR privacy and data management eco-systems. Considering human agency and oversight – limited or absent personalization can restrict users' ability to make informed decisions. Technical robustness and safety – seem challenged by concerns over online data storage, as illustrated by the 'personalization-data-storing' paradox, where efforts to ensure regulatory compliance may conflict with meaningful personalization. In practice, transparency is often operationalized through 'all or nothing' approaches. Lastly, while diversity, non-discrimination, and fairness are increasingly considered in SAR design, older adults are still rarely involved in decisions about data and privacy, limiting the realization of these principles in practice.

5.1. Limitations

While this study sheds light on an overlooked aspect of designing SARs, its main limitation is the use of a small convenience sample. The findings provide valuable insights into developers' and researchers' perspectives. Future research should explore more deeply the perspective of older users to better capture the relational, situational, and temporal complexities of privacy in SARs.

5.2. Conclusion

This study examined how developers and researchers address the tension between personalization and privacy in the datafication processes formed in SARs development for older persons. Looking back at our research questions, we found that in describing the datafication of older persons as SARs users, participants characterized SARs as capable of 'collecting everything.' When contemplating about the concerns this might raise, participants emphasized the users' need for more control, transparency, and personalization, which typically requires personal data and user identification. Finally, we find that older adults are not involved in managing their data and privacy. Using SARs currently entails an 'all or nothing' agreement, leaving older adults with no control over personalizing their datafication.

The 'personalization-data-storing paradox' illustrates these tensions and how it affect users' trust and acceptance. Transparency about data and privacy is important, but formal communication alone may be insufficient if not understandable. To better align with values, such as those presented in the EU trustworthy AI guidelines, this study recommends to accommodate for diverse privacy preferences by allowing users to personalize and control how their data is collected and used. Designing SARs for older persons is particularly prone to marginalization, exclusion, and ageism. The current study demonstrates that this is particularly dominant in the context of privacy and data management. We stress that in order to reduce potential harms from SARs and algorithms while allowing SARs to successfully meet their intended purpose, meaningful involvement of older persons should not be underestimated. While this study recommends applying participatory methods to address these issues, further research is needed to evaluate their effectiveness in increasing explainability, trust, and acceptance.

Acknowledgments

We would like to thank the researchers and designers who shared their experiences with us. We thank Reut Alon for her assistance in the interview process and the validation process of the coding.

Author contributions

CRediT: **Ittay Mannheim:** Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Project administration, Resources, Validation, Visualization, Writing – original draft, Writing – review & editing; **Yael Edan:** Conceptualization, Formal analysis, Funding acquisition, Methodology, Resources, Supervision, Validation, Writing – original draft, Writing – review & editing; **Alexander Peine:** Conceptualization, Formal analysis, Funding acquisition, Methodology, Supervision, Validation, Writing – original draft, Writing – review & editing; **Galit Nimrod:** Conceptualization, Formal analysis, Funding acquisition, Methodology, Resources, Supervision, Validation, Writing – original draft, Writing – review & editing.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work was supported by Ageing in Data (AiD), a research project funded by the Social Sciences and Humanities Research Council of Canada (grant number 895-2021-1020) and housed at Concordia University in Montreal, Canada. It was also supported by Ben-Gurion University of the

Negev through the Agricultural, Biological and Cognitive Robotics Initiative (funded by the Marcus Endowment Fund and the Helmsley Charitable Trust).

Notes on contributors

Ittay Mannheim is a post-doc researcher in the Methodology & Statistics unit of the Institute of Psychology at Leiden University. His research focuses on the intersection of ageing and digital technology. Particularly, Ittay investigates the manifestations of ageism in the use and design of digital technology, in the context of AI, datafication, socially assistive robots, interventions to reduce ageism, and policy implications. His research makes use of a mixed-methods approach, working in trans-disciplinary teams, and using participatory design to promote equality and social change.

Yael Edan (B.Sc. Computer Engineering, 1984; M.Sc. Agricultural Engineering, 1988; Ph.D., Engineering, 1991) is a Full Professor of Industrial Engineering at Ben-Gurion University of the Negev. She specializes in robotics and intelligent automation systems combining the development and application of intelligent automation techniques (sensors, algorithms, and control) with industrial engineering techniques (performance measurement, simulation, systems engineering, and human–robot collaboration and interaction) advancing focused research developments on agriculture robots and social and assistive robots. Personal website: Home | *Yael Edan* Intelligent Robotics Lab (https://smartrobabcbgu.wixsite.com/)

Alexander Peine is a Full Professor of Culture, Innovation and Communication at the Open University of the Netherlands, and a pioneer of the emerging research field of Socio-gerontechnology at the intersection of Science and Technology Studies and Gerontology. He brings a unique expertise in analyzing the social and cultural dimensions of digital innovation and its co-constitution with ageing and later life. He has published more than 50 peer-reviewed articles in leading academic journals, and his TEDx talk on older people as early adopters of technological innovation has attracted over 22,000 views. Alexander was awarded the prestigious Max Weber Postdoctoral Fellowship at the European University Institute and has extensive experience managing large-scale European research projects.

Galit Nimrod Ph.D. is professor at the Department of Communication Studies and a research fellow at the Center for Multidisciplinary Research in Aging at Ben-Gurion University of the Negev, Israel. Dr. Nimrod studies psychological and sociological aspects of leisure, media and technology use among older adults.

Data availability statement

Further information regarding the transcripts' data set and study materials is available upon request from the corresponding author, without compromising the anonymity of the interviewees.

ORCID

Ittay Mannheim http://orcid.org/0000-0003-4304-433X
Yael Edan http://orcid.org/0000-0002-7430-8468
Alexander Peine http://orcid.org/0000-0002-2395-8487
Galit Nimrod http://orcid.org/0000-0001-5878-8222

References

Ananny, M., & Crawford, K. (2018). Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. *New Media & Society*, *20*(3), 973–989. https://doi.org/10.1177/10.1177/1461444816676645

Berridge, C., & Wetle, T. F. (2020). Why older adults and their children disagree about in-home surveillance technology, sensors, and tracking. *The Gerontologist*, *60*(5), 926–934. https://doi.org/10.1177/10.1093/geront/gnz068

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science*, *4*(3), 340–347. https://doi.org/10.1177/10.1177/1948550612455931

Charmaz, K. (2006). *Constructing grounded theory: A practical guide through qualitative analysis*. Sage.

Chuah, S. H.-W., Aw, E. C.-X., & Yee, D. (2021). Unveiling the complexity of consumers' intention to use service robots: An fsQCA approach. *Computers in Human Behavior*, *123*, 106870. https://doi.org/10.1177/10.1016/j.chb.2021.106870

Clark, L., Pantidi, N., Cooney, O., Doyle, P., Garaialde, D., Edwards, J., Spillane, B., Gilmartin, E., Murad, C., & Munteanu, C. (2019). What makes a good conversation? Challenges in designing truly conversational agents. *CHI Conference on Human Factors in Computing Systems Proceedings* (pp. 1–12).

Coghlan, S., Waycott, J., Lazar, A., & Barbosa Neves, B. (2021). Dignity, autonomy, and style of company: Dimensions older adults consider for robot companions. *Proceedings of the ACM on Human-Computer Interaction*, *5*(CSCW1), 1–25. https://doi.org/10.1177/10.1145/3449178

Dalmer, N., Ellison, K., Katz, S., & Marshall, B. (2022). Ageing, embodiment and datafication: Dynamics of power in digital health and care technologies. *International Journal of Ageing and Later Life*, *15*(2), 77–101. https://doi.org/10.1177/10.3384/ijal.1652-8670.3499

De Graaf, M. M., Dragan, A., Malle, B. F., & Ziemke, T. (2021). Introduction to the special issue on explainable robotic systems. *ACM Transactions on Human-Robot Interaction*, *10*(3), 1–4. https://doi.org/10.1177/10.1145/3461597

Diberardino, N., Baleshta, C., & Stark, L. (2024). Algorithmic harms and algorithmic wrongs. *FAccT '24: Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency* (pp. 1494–1511).

Dietrich, M., Krüger, M., & Weisswange, T. H. (2023). What should a robot disclose about me? A study about privacy-appropriate behaviors for social robots. *Frontiers in Robotics and AI*, *10*, 1236733. https://doi.org/10.1177/10.3389/frobt.2023.1236733

European Commission. (2019). *Ethics guidelines for trustworthy artificial intelligence*. Retrieved November 21, 2025, from https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

Felding, S. A., Koh, W. Q., Teupen, S., Budak, K. B., Laporte Uribe, F., & Roes, M. (2023). A scoping review using the Almere model to understand factors facilitating and hindering the acceptance of social robots in nursing homes. *International Journal of Social Robotics*, *15*(7), 1115–1153. https://doi.org/10.1177/10.1007/s12369-023-01012-1

Fosch-Villaronga, E., & Mahler, T. (2021). Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots. *Computer Law & Security Review*, *41*, 105528. https://doi.org/10.1177/10.1016/j.clsr.2021.105528

Gallistl, V., & Von Laufenberg, R. (2024). Caring for data in later life–the datafication of ageing as a matter of care. *Information, Communication & Society*, *27*(4), 774–789. https://doi.org/10.1177/10.1080/1369118X.2023.2279554

Gasteiger, N., Ahn, H. S., Lee, C., Lim, J., Macdonald, B. A., Kim, G. H., & Broadbent, E. (2022). Participatory design, development, and testing of assistive health robots with older adults: An international four-year project. *ACM Transactions on Human-Robot Interaction*, *11*(4), 1–19. https://doi.org/10.1177/10.1145/3533726

Grabler, R., & Koeszegi, S. T. (2025). Privacy beyond data: Assessment and mitigation of privacy risks in robotic technology for elderly care. *ACM Transactions on Human-Robot Interaction*, *14*(1), 1–23. https://doi.org/10.1177/10.1145/3689216

GSA. (2023). Reframing aging journal manuscript guidelines, https://static.primary.prod.gcms.the-infra.com/static/site/gsa/document/Reframing_Aging_Journal_Manuscript_Guidelines.pdf?node=412d7ccc31fac597b9de

Jayaraman, S., Phillips, E. K., Church, D., & Riek, L. D. (2024). Privacy and utility perceptions of social robots in healthcare. *Computers in Human Behavior: Artificial Humans*, *2*(1), 100039. https://doi.org/10.1177/10.1016/j.chbah.2023.100039

Kearney, K. T., Presenza, D., Saccà, F., & Wright, P. (2018). Key challenges for developing a Socially Assistive Robotic (SAR) solution for the health sector. *2018 IEEE 23rd International Workshop on Computer aided Modeling and Design of Communication Links and Networks (CAMAD)* (pp. 1–6).

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134. https://doi.org/10.1177/10.1016/j.cose.2015.07.002

Krupp, M. M., Rueben, M., Grimm, C. M., & Smart, W. D. (2017). Privacy and telepresence robotics: what do non-scientists think? *Proceedings of the Companion of the 2017 ACM/IEEE International Conference on Human-Robot Interaction*.

Lukkien, D. R., Nap, H. H., Peine, A., Minkman, M. M., Moors, E. H., & Boon, W. P. (2025). Responsible scaling of artificial intelligence in healthcare: Standardization meets customization. *Ethics and Information Technology*, *27*(3), 34. https://doi.org/10.1177/10.1007/s10676-025-09842-5

Lutz, C., & Tamó-Larrieux, A. (2020). The robot privacy paradox: Understanding how privacy concerns shape intentions to use social robots. *Human-Machine Communication*, *1*, 87–111. https://doi.org/10.1177/10.30658/hmc.1.6

Maibaum, A., Bischof, A., Hergesell, J., & Lipp, B. (2022). A critique of robotics in health care. *AI & Society*, *37*(2), 467–477. https://doi.org/10.1177/10.1007/s00146-021-01206-z

Mannheim, I., Edan, Y., Alon, R., Peine, A., & Nimrod, G. (2025). Ageism, power, and gaps: Co-designing robots with older adults. *International Journal of Social Robotics*, *17*(11), 2601–2622. https://doi.org/10.1177/10.1007/s12369-025-01325-3

Neven, L. (2010). But obviously not for me': Robots, laboratories and the defiant identity of elder test users. *Sociology of Health & Illness*, *32*(2), 335–347. https://doi.org/10.1177/10.1111/j.1467-9566.2009.01218.x

Peine, A., & Neven, L. (2021). The co-constitution of ageing and technology–a model and agenda. *Ageing & Society*, *41*(12), 2845–2866. https://doi.org/10.1177/10.1017/S0144686X20000641

Rosales, A., & Fernández-Ardèvol, M. (2019). Structural ageism in Big data approaches. *Nordicom Review*, *40*(s1), 51–64. https://doi.org/10.1177/10.2478/nor-2019-0013

Ruckenstein, M., & Schüll, N. D. (2017). The datafication of health. *Annual Review of Anthropology*, *46*(1), 261–278. https://doi.org/10.1177/10.1146/annurev-anthro-102116-041244

Schött, S. Y., Amin, R. M., & Butz, A. (2023). A literature survey of how to convey transparency in co-located human–robot interaction. *Multimodal Technologies and Interaction*, *7*(3), 25. https://doi.org/10.1177/10.3390/mti7030025

Sharkey, A., & Sharkey, N. (2012). Granny and the robots: Ethical issues in robot care for the elderly. *Ethics and Information Technology*, *14*(1), 27–40. https://doi.org/10.1177/10.1007/s10676-010-9234-6

Shelby, R., Rismani, S., Henne, K., Moon, A., Rostamzadeh, N., Nicholas, P., Yilla-Akbari, N. M., Gallegos, J., Smart, A., & Garcia, E. (2023). Sociotechnical harms of algorithmic systems: Scoping a taxonomy for harm reduction. *Proceedings of the 2023 AAAI/ACM Conference on AI, Ethics, and Society*.

Slane, A., & Pedersen, I. (2025). Bringing older people's perspectives on consumer socially assistive robots into debates about the future of privacy protection and AI governance. *AI & Society*, *40*(2), 691–710. https://doi.org/10.1177/10.1007/s00146-024-01894-3

Søraa, R. A., Tøndel, G., Kharas, M. W., & Serrano, J. A. (2023). What do older adults want from social robots? A qualitative research approach to human-robot interaction (HRI) studies. *International Journal of Social Robotics*, *15*(3), 411–424. https://doi.org/10.1177/10.1007/s12369-022-00914-w

van Leersum, C. M., & Peine, A. (2025). Only practical knowledge or knowing the algorithm? Notions and necessities of explainable artificial intelligence in long-term care. *AI & Society, 41*, 1189–1206.

Waldman, A. E. (2020). Cognitive biases, dark patterns, and the 'privacy paradox'. *Current Opinion in Psychology*, *31*, 105–109. https://doi.org/10.1177/10.1016/j.copsyc.2019.08.025

Weitz, K., Schiller, D., Schlagowski, R., Huber, T., & André, E. (2019). "Do you trust me?" Increasing user-trust by integrating virtual agents in explainable AI interaction design. *Proceedings of the 19th ACM International Conference on Intelligent Virtual Agents*. https://doi.org/10.1177/10.1145/3308532.3329441

Xu, K., Chen, X., Liu, F., & Huang, L. (2025, October). What did you hear and what did you see? Understanding the transparency of facial recognition and speech recognition systems during human–robot interaction. *New Media & Society, 27*(10), 5776–5802.

Zafrani, O., & Nimrod, G. (2019). Towards a holistic approach to studying human–robot interaction in later life. *The Gerontologist*, *59*(1), e26–e36. https://doi.org/10.1177/10.1093/geront/gny077

Zafrani, O., Nimrod, G., & Edan, Y. (2023). Between fear and trust: Older adults' evaluation of socially assistive robots. *International Journal of Human-Computer Studies*, *171*, 102981. https://doi.org/10.1177/10.1016/j.ijhcs.2022.102981

Zhang, W., Yin, J., Chan, K. I., Sun, T., Jin, T., Jeung, J., & Gong, J. (2024). Beyond digital privacy: Uncovering deeper attitudes toward privacy in cameras among older adults. *International Journal of Human-Computer Studies*, *192*, 103345. https://doi.org/10.1177/10.1016/j.ijhcs.2024.103345

Zhu, H., & Zhang, M. (2025). "I don't get it, but I accept it" exploring uninformed consent to privacy policies: A neutralization perspective. *Computers & Security*, *153*, 104396. https://doi.org/10.1177/10.1016/j.cose.2025.104396

Appendix: Full lists of themes, categories, and codes.

Theme 1: 'The robot collected everything': datafication in SARs for older persons								
Digital engagement & interaction	Acceptance	Face recognition & visual	Positioning monitoring and movement	Social network & emotional	Research	Health	Language, communication & audio	Activities & Gamification
active engagement (frequency)	satisfaction	facial expression or recognition	distancing	family time	qualitative interview	Hand grip/pressure	choice of words, language, text	frequency of functionalities/ experiences
interactions	pleasurable	visual/ video recording	gait/kinematic	social and personal information shared	qualitative observational	impairment	sound/voice	level achieved (cognitive game)
usage data	willingness to use	Eye contact with the robot	mapping	contacts	questionnaires	sleep	Questions about the robot	
robot task efficiency	trust		monitoring	emotions		health variables		
User task success	acceptance/ rejection		movement (not video)			eating		
time of use			position			wearables recording physiological data		
safety								
interface								
Reminders								

Theme 2: Legal frameworks 'all or nothing'				
Data regulations	Compliance and Consent	Control over the data	Ownership and access	Data collection & storage
AI regulations and consequences	Consent signed about data and privacy	Controlling data recording settings – everything or nothing	Company owns the data	The robot collected everything (data)
Data anonymized	Consent to different aspects	Controlling data recording settings by researcher	No access to the data used by google recognition	Robot didn't collect any data
Privacy policy & regulations	Understanding what the consent means? Privacy ethics	Control of the robot and agency	open code	Data stored in university laptops
	Generational differences in consent			Data collected locally (offline) and not stored between sessions
	Consent from legal guardian			No video data due to privacy
	No full consent – no product			Data storing paradox

Theme 3: Perceptions of data usage, concerns, and personalization					
Older persons don't care about data and privacy	Concerns about privacy	Transparency	Requirements for data design	Personalization / customization	Data for learning and design
People don't care about data collected about them	Concerns about privacy – surveillance, listening or watching	Transparency and clarity of data collected, use, and access	Clear privacy related data button	Personalization	Data informing the design
Older persons fine with recording data for research	AI development – negative implications of data use	Transparency, communication, and acceptance	Master button	Personalization – control over privacy	Data is really one of the best ways to learn. It's just unsolicited
	Feel safe that data is protected		A robot that does not run facial recognition cannot be a social robot	Personalization – start key word	Machine learning to imitate behavior
	Violation of safeguards			Personalization and stigmatization	Biased data – Not big data
	Beware of deception and Media representation of robots			Data personalization can increase the benefit	Modelling the human
	Connecting online comes with a responsibility			Customization for the client by the robot manufacturer	AI will actually be alive
				Personalization to support performance	
				Personalized feedback and communication	