Evaluating the Impact of a Personal Data Communication Policy in Human-Robot Interactions

Lewis Riches
Robotics Research Group
University of Hertfordshire
College Lane, UK
email: l.riches@herts.ac.uk

Kheng Lee Koay
Robotics Research Group
University of Hertfordshire
College Lane, UK
email: k.l.koay@herts.ac.uk

Patrick Holthaus
Robotics Research Group
University of Hertfordshire
College Lane, UK
email: p.holthaus@herts.ac.uk

***Abstract*—Personal companion robots are increasingly integrated into households, offering tailored experiences through personalisation. However, using multiple communication pathways heightens the risk of inadvertent personal data exposure. This paper presents a novel communication policy designed to mitigate such risks by dynamically adjusting communication strategies based on the sensitivity of the shared data. We measure participant preferences for these adaptive communication methods through empirical assessment. Our findings indicate that the proposed policy effectively minimises personal data exposure, fostering increased trust in the robot's handling of sensitive information.**

Keywords-Personalisation; Personal Data Communication; Human-Robot Interaction; Perceptions Of Privacy

I. Introduction

Health care assistance [1], butler services [2], and educational tutors [3], the roles a companion robot could take within a person's home are starting to be explored in research. Leveraging techniques such as personalisation, social companion robots can learn from the user and adapt their behaviour to provide a unique and custom experience [4]. Regardless of their role within the home, these robots will need to communicate with the user. As such, research within this field has brought about a multitude of different communication pathways, including audible [5], visual [6] and sign language [7], to name but a few. Using these communication methods, social companion robots can personalise their communication method and topic of communication to the user. While multimodal communication pathways are vital, such methods increase the risk of personal data exposure, as identified by Calo [8].

With access to the private space of a home, along with personalisation techniques, social companion robots have easy access to sensitive and personal data about their user. A robot's ability to communicate personal data is akin to that of humans. Robots need to have social awareness, understand the relationship between people, what type of personal data they are communicating, and the impact of exposing such personal data within the context. Unlike Human-Computer Interaction (HCI), where a device needs to be unlocked [9] or have some form of user intervention to communicate personal data. However, to put manual intervention into social companion robots before they can communicate anything would impede the natural communication experience a robot would provide.

A simple solution to fix these communication issues would be to prevent the robot from entering private spaces within the home [8], control what personal data it can collect through sensors [10] and give it limited personal data. However, such techniques hamper the functions of personalisation. Butler et al. [11] and Klow et al. [12] show that people are willing to give up more sensitive personal data to gain benefits and functions. These tradeoffs mean people want to give a robot their personal data to get personalised features and tasks done in specific ways, even with the added risk of exposure through communication. For example, giving a robot your medical information to enable features such as medication reminders or the robot adapting its communication style if you have hearing loss. Withholding essential personal data required for personalisation features due to concerns about data exposure is similar to denying a chef access to a kitchen out of fear of hazards. Instead, we propose to put policies in place at the communication layer of the robot to protect personal data.

Within HRI, there are currently limited communication strategies for addressing this. An approach put forward by Marchang et al. [13] is to use a blockchain approach, where only authorised personnel can be present for the robot to communicate personal data. Such a technique is viable in HCI but requires manual intervention (Face ID), impeding natural communication. A common approach used within research studies is to use consent forms that do not require a communication policy and either use fake personal data for the participant or use only authorised personal data. For example, Di Napoli et al. [14] turn off video recording and skeletal tracking to ensure that only the desired personal data is collected. While ethically sound, both approaches lack consideration for how the robot would need to communicate in the real world.

In a real-world domestic setting, a robot needs to understand what it is saying to be able to assess if it is appropriate to say within a specific context. This means understanding the sensitivity of the personal data, the people within a given context, and the impact of sharing the personal data within that context. Findings from [15] [16] show that the sensitivity of different personal data items is different. Both works also show that personal differences can also influence these perceived sensitivities.

This work looks at how a communication policy could use

perceptions of personal data sensitivity to determine how to communicate personal data. In particular, this work takes the classification of personal data by Riches et al. [16] and applies a different communication style for low, medium and high-concern personal data. Within this work, we want to explore if such a policy provides appropriate and safe communication of personal data while building trust in the robot's ability to handle personal data. For this purpose, this work aims to answer the following research questions:(**RQ1**) Can a communication policy based on the concern of personal data exposure (personal data concern classification) positively influence people's views on a robot's communication of personal data (e.g. convenient, helpful and trustworthy)? (**RQ2**) How does such a communication policy influence people's trust towards the robot compared to no communication policy? (**RQ3**) Does such a policy provide a more appropriate way for a robot to communicate personal data to the user in different social contexts when a third party is present? Section II presents the design and implementation of a hybrid study, while the results are analysed in Section III. The implications of the findings for Human-Robot Interaction (HRI) are discussed in Section IV, followed by the conclusion in Section V.

II. Methodology

The study presented in this paper comes from an ethically approved hybrid study, which was conducted both online (aSPECS/PGR/UH/05388) and in person (aSPECS/PGR/UH/05389). These studies had a robot communicating three pre-determined personal data reminders created for the study to the participant in front of a third party. It was decided to do an online and in-person version of this study to see if there was a difference in participant perceptions when experiencing the interactions in person compared to seeing it online through a video. The reminders communicated by the robot were chosen to cover the three classifications of concern found by Riches et al. [16]: Low (Preferences), Medium (Political opinions) and High (Financial Records). The full wording of the reminders was:

- Preferences (Low Concern): "Your favourite TV program, the NFL, is on tomorrow, and you enjoy eating cookies and drinking coke while watching this. Would you like me to add this to your shopping list?"
- Political Opinions (Medium Concern): "You need to renew your membership for the Orange Political Party as it expires next week, and there are key votes happening in the coming months. Would you like me to renew this for you now?"
- Financial Records (High Concern): "Your phone bill is due today, totalling £60. You need to pay this as you have been late on this for the last few months. Would you like me to pay this for you now?"

The scenario narrative was that the participant was in their home, and a neighbour came around for a chat. The participant and neighbour were sitting at the dining room table having a drink when the robot came to the participant with a few personal data reminders. For this study, we had two scenarios: a trusted neighbour scenario and a new neighbour scenario. We defined a trusted neighbour as someone the participant had known for 5-plus years and looked after their house when the participant went on holiday. We defined a new neighbour as someone the participant had never met before and had only moved in a day ago. In each scenario, we had two conditions.

The **control condition** was where the robot used no communication policy, saying all three personal data reminders out loud. The **experimental condition** was where the robot used our classification policy to communicate all three reminders. Our classification policy communicated personal data based on the sensitivity of the personal data [16] within the reminder. Low-concern personal data was said out loud in full; for medium-concern personal data, the robot asked the user whether they wanted it said out loud or sent to their phone; for high-concern personal data, these were sent directly to the user's phone.

The robots used in the studies were different. The online study used the Humanoid Pepper [17] robot along with the Non-Humanoid Fetch [18] robot. We chose these two robots to see if their anthropomorphism influenced participants' perceptions of the robot handling and communicating their personal data. We only used Fetch for the in-person study as the Pepper robot could not navigate reliably. This is to avoid participant's responses being influenced by the robot's navigation abilities. For the in-person study, the University of Hertfordshire Robot House [19] was used to provide a realistic domestic setting to immerse participants in the story.

A. Procedure

For both studies, participants first completed a pre-trial questionnaire. This questionnaire collected participants' age, gender, smart assistant use, Ten Item Personality Index (TIPI) [20], Negative Attitudes Towards Robotics (NARS) [21], and experience with robotics. The final question of this section aimed to understand participants' perceptions of approval for a robot to know and store the thirteen items of personal data classified in [16]. The question provided a picture and description of the robot, then asked, "Please rank your approval of <Fetch or Pepper> collecting and storing the following personal data for generating and communicating tailored reminders." Participants rated this approval on a 5-point Likert scale from Strongly disapprove to Strongly approve. For the in-person study, only fetch was used, and participants also had the chance to interact with Fetch physically and see how it moves and communicates before answering this question. For the online study, the robot the participants experienced was between-subject and randomised which robot they experienced.

1) Online: The online study focuses on the preferred communication policy in the presence of a third party (not focusing on the relationship between the user and the third party) and whether the robot's appearance (pepper and fetch) influences the participant's preferences.

After the pre-trial questionnaire, participants watched two videos and answered the post-condition questionnaire after

each video. Each video showed one of the two conditions (Communication policy used). The order in which these were shown was randomised and counterbalanced, so the order did not influence participants' perceptions. The videos were filmed in first person as if the participant was experiencing them, akin to the in-person study. For the scenario (neighbour type) of the videos, no details were given in the videos about who the third party was. This detail was asked in the post-condition questionnaire.

2) In-Person: The in-person study focuses on the third party present and their relationship to the user. It allows participants to imagine themselves in the role and act with the third party as if it were their neighbour (new or trusted).

After the pre-trial questionnaire, participants participated in one scenario (neighbour type) with two conditions (communication policy). This meant the participant acted twice, once with the robot using the control policy (no communication policy) and once with it using the experimental policy (classification communication policy), with both times being with the same neighbour (new or trusted). The scenario chosen for each participant was randomised and counterbalanced, and the order of the conditions was counterbalanced. After each interaction, participants would then complete a post-condition questionnaire.

The post-condition questionnaire consisted of four questions. Firstly, participants were asked, "Based on how it communicated your reminders in this interaction, would you trust the robot's ability to provide reminders while keeping your personal data secure?" choosing either yes or no and giving a qualitative reason. The second question asked, "Based solely on the interaction, please rank your approval of <Fetch or Pepper> collecting and storing the following personal data for generating and communicating tailored reminders as it did in the interaction." participants rated this on a 5-point Likert scale from Strongly disapprove to Strongly approve for all 13 personal data items identified previously from [16]. Question three was different between the two studies. The online study was split into two parts and asked about each neighbour: "Please rank your approval of how the robot communicated each reminder if the neighbour present was a <new or trusted> neighbour.". The in-person study asked, "Please rank your approval of how the robot communicated each reminder in front of your neighbour.". For both studies, participants rated these on a 5-point Likert scale from Strongly disapprove to Strongly approve for each of the three personal data reminders listed previously. The final question asks, "Please rank whether you agree or disagree with the following statements and explain your rankings" with participants rating their agreement on a 5-point Likert scale from Strongly disagree to Strongly Agree for three statements. The statements were, "I am happy with the way the robot communicated my personal data", "My personal data is safe when the robot communicates my reminders to me", and "The way the robot communicated my personal data was natural".

B. Participants

In total, we collected responses from 220 participants. Of the 182 participants in the online study, 89 self-identified as male and 93 self-identified as female, with a median age of 35 and a range of 18 - 84. Of the 38 participants in the in-person study, 20 self-identified as male and 18 as female, with a median age of 27 and a range of 19 - 51.

III. Results

In this paper, we performed two studies, one online and one in-person. Using Mann-Whitney U tests, we found no statistical difference between the results from both studies. As such, the results in this paper will report the combination of both studies. While the online study used two different robots, whereas the in-person study only used one, there were also no statistical differences between these, meaning we were able to combine the results.

A. Effect of a communication policy on perceptions of trust

Participants were asked which communication protocol they would prefer to use in daily life. 84% of participants chose the experimental policy, with the remaining 16% choosing neither and no participants choosing the control policy. When asked, "Would you trust the robot's ability to provide reminders while keeping your personal data secure?" 85% of participants said no, and 15% said yes for the control policy, with 14% saying no and 86% of people saying yes for the experimental policy. This difference in trust rating was statistically significant ($Z = -13.92$, $p =< .001$). On giving reasons for their rating, the main themes for not trusting the control policy were feeling their personal data was unsecured, having no control over their personal data and feeling uncomfortable with their personal data being exposed (see examples below):

- Unsecured
  - "The robot's speech did not uphold the safety of my data."
  - "I didnt feel like my personal data is secure. So I couldn't trust the robot with my personal details"
- No Control
  - "The absence of control over my data was a glaring issue."
  - "I have no control over the reminders or what the robot says"
- Uncomfortable
  - "It just felt uncomfortable when the robot mentioned the orange party. Even if the political party I am a member of is known. I would not like this kind of information to be revealed to a new neighbour. Also, the phone not being paid can be embarrassing."

In the reasoning given for why participants trusted the experimental policy, the two main themes were the robot asking for consent and not saying highly sensitive information out loud (see examples below):

- Asking for Consent

  - ”Having different levels of security on different aspects of data felt reassuring. Especially being able to choose on some of the data.”
  - ”The robot asked for consent first to say it out loud/sent as a text message. This part of interaction helped to build trust.”
  - ”The robot waited for my consent before disclosing any personal information that’s why I trust the robot’s ability to keep my data secure.”
- Not saying Sensitive information out loud
  - ”Sending reminder to my phone is a really good idea comparing to saying them loudly”
  - ”Using the notification based approach is perfect saving the sensitive data issue”

Participants were asked to rate their agreement with two statements for each of the communication policies:

- I am happy with the way the robot communicated my personal data
- My personal data is safe when the robot communicates my reminders to me

For the control policy, 81% of participants disagreed with being happy with the way the robot communicated their personal data, and 85% disagreed with their personal data feeling safe when the robot communicated it. For the experimental policy, 68% agreed with being happy with the way the robot communicated their personal data, and 78% agreed with their personal data feeling safe when the robot communicated their personal data. The central theme of why participants agreed or disagreed with these statements was the fact the robot did or did not say the personal data out loud (see examples below):

- Disagree
  - ”It revealed potentially sensitive data to another person”
  - ”I feel that fetch, although said what he wanted to remind me of, he went into too much detail in front of my new neighbour. ”
  - ”It could have omitted the sensitive information from the reminder rather than just saying it all out”
- Agree
  - ”Sending financial reminders to my phone meant it felt safe and under my control. I was not worried it would reveal sensitive information.”
  - ”It has classified senstive data and only voiced out non-senstive data and it was able to send a notification for the sensitive data”
  - ”I liked that it could use my phone to send me the reminder rather then just saying everything out loud”

Participants were asked, “Please rank your approval of <Fetch or Pepper> collecting and storing the following personal data for generating and communicating tailored reminders”. This was done before experiencing any scenarios (pre) and after experiencing each communication policy with the same assigned robot (Fetch or Pepper). For all personal data items other than preferences, the approval for the robot

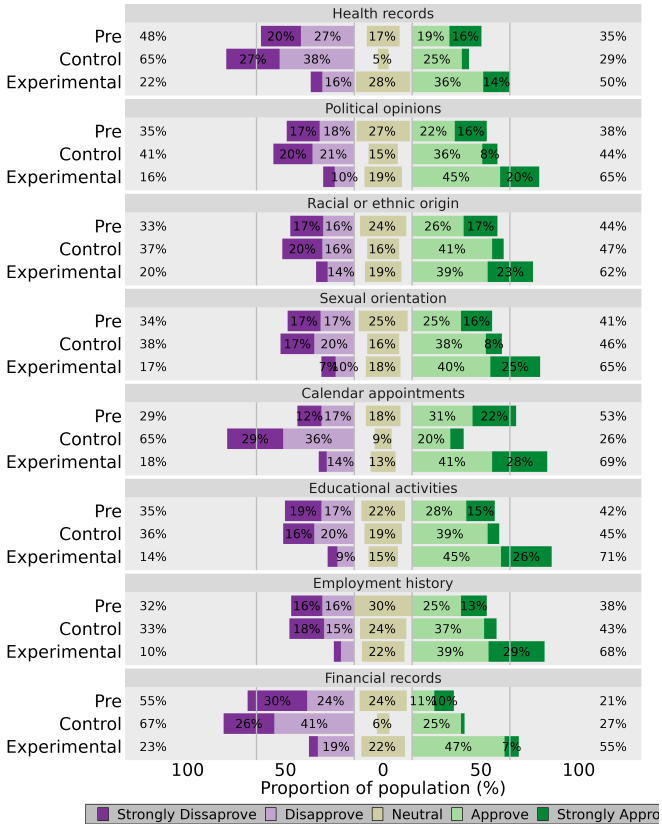

Figure 1. A bar graph showing the distribution of participants’ ratings for a robot to know and store personal data items.

to know and store the personal data after demonstrating the experimental policy was higher than the control policy and initial perceptions. The results of this question are shown in figure 1.

Using Mann-Whitney U tests the difference between the pre-approval and approval for the experimental policy was statistically significant for Health records ($z = -4.17$, $p =< .001$), Political opinions ($z = -5$, $p =< .001$), Educational activities ($z = -6.15$, $p =< .001$), Sexual orientation ($z = -5$, $p =< .001$), Racial or ethnic origin ($z = -3.82$, $p =< .001$), Financial records ($z = -7.54$, $p =< .001$), Employment history ($z = -6.74$, $p =< .001$), and Calendar appointments ($z = -3.2$, $p = 0.001$). In all cases, approval increased for the experimental policy over the pre-approval ratings.

Using Mann-Whitney U tests, the difference between the approval for the control policy and the experimental policy was statistically significant for Health Records ($z = -7.9$, $p =< .001$), Political opinions ($z = -5.92$, $p =< .001$), Educational activities ($z = -7.09$, $p =< .001$), Sexual orientation ($z = -5.65$, $p =< .001$), Racial or ethnic origin ($z = -5.23$, $p =< .001$), Financial records ($z = -8.53$, $p =< .001$), Employment history ($z = -7.17$, $p =< .001$), and Calendar appointments ($z = -10.21$, $p =< .001$). In all cases, approval increased for the experimental policy compared to the control policy.

Using Mann-Whitney U tests, the difference between the pre-approval and the approval for the control policy was statistically significant for Health records ($z = 3.35$, $p = 0.001$) and Calendar appointments ($z = 7.15$, $p =< .001$). In both cases, approval decreased for the control policy compared to the pre-approval rating.

Comparing the change in approval between the control policy and experimental policy showed a split based on the sensitivity of the personal data. Approval change between control policy and experimental policy for medium concern personal data items (Political Opinions, Racial or Ethnic Origin, Sexual Orientation, Educational Activities, and Employment History) had a 21% to 25% decrease in disapproval ratings, while neutral ratings changed by -4% to 4%, and approval ratings increased by 21% to 26%. Approval change for High Concern personal data (Health Records, Calendar Appointments, and Financial Records) had a disapproval decrease of 41% to 47%, while neutral increased by 4% to 23%, and approval increased by 21% to 43%.

B. Perceptions of Personal Data Reminder Communication

Participants were asked to rate their approval of how the two communication policies communicated the three personal data reminders. These ratings are shown in figure 2. The figure shows that for all three reminders, approval for the experimental policy was higher than approval for the control policy.

Using Mann-Whitney U tests the approval rating for the two policies when a **new** neighbour is present was found to be statically significant for all three personal data reminders: Phone Bill ($z = -12.91$, $p =< .001$), Political Party ($z = -12.82$, $p =< .001$), and Preferences ($z = -4.08$, $p =< .001$). When a **trusted** neighbour was present, there were also statistically significant differences between the approval of both communication policies: Phone Bill ($z = -9.85$, $p =< .001$), Political Party ($z = -9.53$, $p =< .001$), and Preferences ($z = -2.28$, $p = 0.023$). In all cases, approval increased for the experimental policy compared to the control policy.

For the control policy, there was no statistical difference between participants' approval ratings by neighbour type for all three reminders. However, a slight trend is shown, with approval for the trusted neighbour being higher than for the new neighbour, showing some influence of the neighbour type on the approval rating. For the control communication policy, the approval for the Phone Bill reminder had majority disapproval for both neighbours, with 64% disapproval for the trusted neighbour and 72% for the new neighbour. The preferences reminder has majority approval for both neighbour types, with 82% approval for a trusted neighbour and 76% for a new neighbour. For political opinions, the approval ratings are split over approve, neutral and disapprove, showing participants' ambivalence for this reminder. Political opinions have 41% disapprove, 26% neutral, and 31% approve of a trusted neighbour, 47% disapprove, 29% neutral, and 22% approve of a new neighbour.

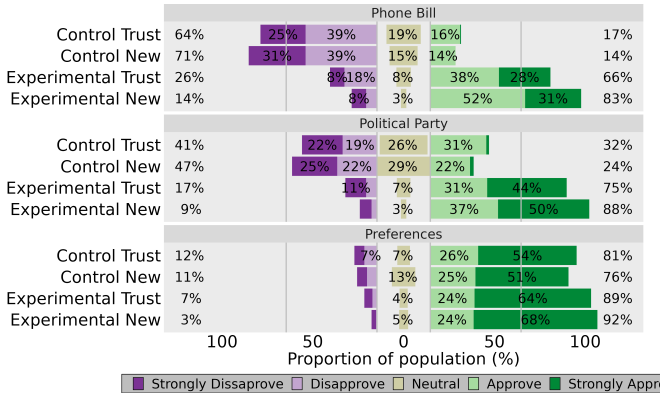

Figure 2. A bar graph showing the distribution of approval ratings for the different personal data reminders.

For the experimental policy, approval ratings for the neighbour types were found to be statistically different using Mann-Whitney U tests for Phone Bill ($Z = -2.31$, $p = .021$) and Political Party ($Z = -2.18$, $p = .029$) reminders. In both cases, approval ratings decreased for a trusted neighbour compared to a new neighbour. Approval drops by 17% for the phone bill reminder and 13% for the political party reminder. While approval drops, both neighbour types have a majority approval for the experimental policy. Phone bill has an overall approval rating of 66% for a trusted neighbour and 83% for a new neighbour, while Political Party has an approval rating of 75% for a trusted neighbour and 88% for a new neighbour.

In participants' qualitative responses, the common theme as to why approval was lower for a trusted neighbour was that they felt like they were hiding information from the neighbour. This is because when the robot notifies the user of a medium or high concern reminder, it still says the personal data item but does not go into detail. For example, political opinions are a medium concern personal data, so the robot would say, "I have a reminder about your political opinions would you like this saying out loud?". This caused participants to feel uncomfortable as the third party heard that they had a reminder on this but could not know what it was about. Participants gave feedback that instead of saying the personal data item in the reminder, the robot could instead say a generic statement such as "I have an important reminder for you".

IV. Discussion

This work presents a hybrid study conducted online and in person. This work aimed to see how a communication policy based on the classification of personal data exposure sensitivity [16] is perceived when used to communicate personal data reminders in front of a neighbour. We manipulated the neighbour type, either being a new or trusted neighbour.

Our approach presented was to use a classification-based communication policy. This policy uses the sensitivity of the personal data being communicated to adapt how it communicates the reminder. **RQ1** wanted to see if such a policy positively influenced views on a robot communicating personal

data. The results presented show that the majority of participants were very happy with the robot communicating using this classification policy while feeling their personal data was secure with the robot.

RQ2 aimed to understand if a communication policy could influence trust in the robot communicating personal data. Our findings suggest that trust is influenced by the communication policy. The majority of participants (86%) said they would trust our classification policy to provide reminders using personal data while keeping the personal data secure. When participants were asked if they trusted the control policy, 85% said they would not trust it to keep their personal data secure while communicating it. The results also show that after experiencing our communication policy, participants were more approving of a robot knowing and storing personal data items. Further, after experiencing the control policy, the disapproval rating increased for the robot to know and store personal data items. This means that through the display of the classification policy alone, trust is built between the user and the robot to handle personal data.

RQ3 looked at whether a classification communication policy could appropriately communicate personal data when a third party is present. For all three personal data reminders, the classification policy had a majority approval for communicating the personal data. However, when comparing this approval between neighbour types, approval decreased for a trusted neighbour compared to a new neighbour. Participants' reasons for this were that saying the topic of the communication made it seem like they were hiding something from their neighbour. Instead, a more generalised statement could be used while still notifying users of a reminder that needs their attention.

Our results found no influence of the robot's anthropomorphism (Humanoid or Non-Humanoid) on participants' approval ratings. These results agree with the findings from Rossi et al. [22], who found that a robot's appearance does not influence the trust of a robot to have personal data.

V. Conclusion

The classification policy presented in this work increased the participant's approval of the robot knowing and storing personal data for personalised communication. These results show that demonstrating secure communication of personal data improves users' trust in the robot having the personal data. For HRI, this means that instead of inhibiting personalisation by not allowing the robot access to personal data, the robot can demonstrate secure personal data communication. This approach would allow personalisation to be uninhibited, removing the need for users to make privacy trade-offs for personalisation gains [11] [12].

References

[1] H.-M. Gross *et al.*, "Robot companion for domestic health assistance: Implementation, test and case study under everyday conditions in private apartments," in *2015 IEEE/RSJ IROS*, 2015, pp. 5992–5999.

[2] M. M. A. de Graaf and S. Ben Allouch, "The evaluation of different roles for domestic social robots," in *2015 24th IEEE RO-MAN*, 2015, pp. 676–681.

[3] D. Leyzberg, S. Spaulding, and B. Scassellati, "Personalizing robot tutors to individuals' learning differences," in *Proceedings of the 2014 ACM/IEEE HRI*. ACM, 2014, pp. 423–430.

[4] W. Ho, K. Dautenhahn, M. Y. Lim, and K. Du Casse, "Modelling human memory in robotic companions for personalisation and long-term adaptation in hri." in *Frontiers in Artificial Intelligence and Applications*, vol. 221, 01 2010, pp. 64–71.

[5] M. Heckmann and A. Richter, "Assistance system and method for providing information to a user using speech output," Germanys Patent EP3 772 735, Feb. 10, 2021.

[6] K. L. Koay *et al.*, "Hey! there is someone at your door. a hearing robot using visual communication signals of hearing dogs to communicate intent," in *2013 IEEE ALife*, 2013, pp. 90–97.

[7] P. Uluer, N. Akalın, and H. Köse, "A new robotic platform for sign language tutoring," *International Journal of Social Robotics*, vol. 7, no. 5, pp. 571–585, Nov. 2015.

[8] R. M. Calo, "Robots and privacy," in *Machine Ethics and Robot Ethics*. Routledge, 2020, ch. 33, pp. 491–505.

[9] C. Bhagavatula *et al.*, "Biometric authentication on iphone and android: Usability, perceptions, and influences on adoption," *Proceedings 2015 Workshop on Usable Security*, pp. 1–10, 2015.

[10] J. Klow *et al.*, "Privacy, utility, and cognitive load in remote presence systems," in *11th ICSR*. Berlin, Heidelberg: Springer-Verlag, 2019, pp. 730–739.

[11] D. J. Butler, J. Huang, F. Roesner, and M. Cakmak, "The privacy-utility tradeoff for remotely teleoperated robots," in *2015 10th ACM/IEEE International Conference on Human-Robot Interaction (HRI)*, 2015, pp. 27–34.

[12] J. Klow *et al.*, "Privacy, utility, and cognitive load in remote presence systems," in *Proceedings of the Companion of the 2017 ACM/IEEE International Conference on Human-Robot Interaction*, ser. HRI '17. New York, NY, USA: Association for Computing Machinery, 2017, pp. 167–168.

[13] J. Marchang and A. Di Nuovo, "Assistive multimodal robotic system: Security and privacy issues, challenges, and possible solutions," *Applied Sciences*, vol. 12, p. 2174, 2022.

[14] C. Di Napoli, G. Ercolano, and S. Rossi, "Personalized home-care support for the elderly: a field experience with a social robot at home," *User Modeling and User-Adapted Interaction*, vol. 33, no. 2, pp. 405–440, Apr 2023.

[15] A. Rossi, G. Perugia, and S. Rossi, "Investigating customers' perceived sensitivity of information shared with a robot bartender," in *Social Robotics: 13th International Conference, ICSR 2021, Singapore, Singapore, November 10-13, 2021, Proceedings*. Berlin, Heidelberg: Springer-Verlag, 2021, pp. 119–129.

[16] L. Riches, K. L. Koay, and P. Holthaus, "Classification of personal data used by personalised robot companions based on concern of exposure," in *Social Robotics*. Cham: Springer Nature Switzerland, 2022, pp. 228–237.

[17] Aldebaran, "Pepper." [Online]. Available: https://www.aldebaran.com/en/pepper [retrieved: April, 2024]

[18] Zebra, "Autonomous mobile robots." [Online]. Available: https://www.zebra.com/us/en/products/autonomous-mobile-robots.html [retrieved: April, 2024]

[19] P. Holthaus, "Robot house." [Online]. Available: https://robothouse.herts.ac.uk/ [retrieved: April, 2024]

[20] S. D. Gosling, P. J. Rentfrow, and W. B. Swann, "A very brief measure of the big-five personality domains," *Research in Personality*, vol. 37, pp. 504–528, 2003.

[21] T. Nomura, T. Suzuki, T. Kanda, and K. Kato, "Measurement of negative attitudes toward robots," *Social Behaviour and Communication in Biological and Artificial Systems*, vol. 7, pp. 437–454, 2006.

[22] A. Rossi, K. L. Koay, and S. Rossi, "Evaluating people's perception of trust and privacy based on robot's appearance," in *2023 32nd IEEE International Conference on Robot and Human Interactive Communication (RO-MAN)*, 2023, pp. 1928–1933.