Honda Research Institute EU
Honda Research Institute Europe GmbH
https://www.honda-ri.de/

Effective Engineering, Stakeholder Involvement, and Regulatory Plurality within Privacy-Aware Robotics

Leigh Levinson, Manuel Dietrich, Alan Sarkisian, Selma Šabanovi?, William Smart

2025

Preprint:

This is an accepted article published in 20th ACM/IEEE International Conference on Human-Robot Interaction (HRI 2025). The final authenticated version is available online at: https://doi.org/10.1109/HRI61500.2025.10974108
Copyright 2025 IEEE

Effective Engineering, Stakeholder Involvement, and Regulatory Plurality within Privacy-Aware Robotics

Leigh Levinson
Indiana University Bloomington
Bloomington, Indiana, United States
0000-0002-6964-8441

Manuel Dietrich
Honda Research Institute Japan Co. Ltd.
Wako, Japan
0000-0001-6819-8656

Alan Sarkisian
Honda Research Institute Japan Co. Ltd.
Wako, Japan
0000-0001-5965-0735

Selma Šabanović
Indiana University Bloomington
Bloomington, Indiana, United States
0000-0002-2553-854X

William D. Smart
Oregon State University
Corvallis, Oregon, United States
0000-0001-6867-5125

***Abstract*—Privacy is an important yet understudied focus in consideration of successful human-robot interaction (HRI). In this paper, we present a thematic analysis of the topics discussed in the Privacy-Aware Robotics Workshop held at the HRI Conference in 2024. The analysis points across the perspectives of User, Engineering, and Society with particular identification of open "interdisciplinary zones" at the intersections of these perspectives. Based on that, we formulate and present three main themes for future research directions: the tension between robot functioning and effectiveness of privacy implementations in real-world contexts; the need to involve and empower target user communities in the co-design of privacy-aware robots, and the consideration of regulatory frameworks that extend across jurisdictions in robot design.**

***Index Terms*—Privacy, Security, Explainability, Co-Design, Contextual Integrity**

I. Introduction and Background

As robots become more integrated into human environments, they must navigate both physical and social realms. To act successfully in these socially rich environments, they will need to be keenly aware of their physical and social surroundings and the people within it. This awareness, however, requires the collection of personal data, including potentially sensitive information, making a privacy-sensitive design towards the responsible handling of personal data a crucial factor for user acceptance.

Privacy is typically approached from one or more of the following perspectives: legal dimensions varying across global jurisdictions [13], ethical aspects encompassing human autonomy and "the right to be left alone" [41], informational (in)justice [39], psycho-sociological considerations encompassed in "privacy as contextual integrity" [23] and communication boundary management theories [26]. Recognized dimensions of privacy that are further affected by context are psychological, physical, decisional, and informational privacy [34]. Robots in everyday contexts touch on many of these dimensions [19], [10]. Through the robot's social character, they may be entrusted with sensitive information, particularly when users develop emotional relationships with the artificial entity [19], [9]. With this, robots additionally influence social dimensions of privacy [21] placing robots in unique ontological positions in compared to a person's other social relationships.

Although current research on human-robot interaction increasingly explores scenarios involving everyday environments [32], real-world privacy challenges remain largely underexplored. Social robot uses in unconstrained environments may involve people who have not agreed to data processing or access to their spaces [5].

To spark a broader discussion addressing this research gap, a workshop titled "privacy-aware Robotics" was held at the ACM/IEEE International Conference on Human-Robot Interaction (HRI) 2024 to foster interdisciplinary dialogue on this critical issue. The overall goal was to allow participants to explore and identify topic areas and research questions surrounding privacy-aware robots as a follow-up to previous conversations that arose from the 2017 workshop on privacy-sensitive robotics [30]. Specifically, we invited contributions that aligned with at least one of the following themes:

- User: What are the dynamic privacy needs of users in everyday social environments? How do these interactions and the boundaries users draw inform the development of robotic applications?
- Engineer: What are the engineering limitations to privacy-aware robotics in information-rich environments and what are some potential solutions?
- Society: What are the broader legal and ethical privacy challenges for social robotics research and adoption, considering transparency, consent, and intervention?

First, we will introduce the structure and key contributions of keynotes, panelists, participant talks and interactive sessions. Then, we systematically map discussion points and questions from the workshop to highlight how these themes manifest in the field and should inspire future directions. As such, the contribution of this paper is two-fold:

- Presentation of privacy-aware robotics discussion points

across the User, Engineering, and Society perspectives with particular identification of open "interdisciplinary zones" at the intersections of these perspectives.
- Formulation of major themes for inspiring future research directions based on the insights gained from the analysis.

II. Workshop

The workshop began with a conceptual introduction, followed by keynotes from Dr. Sanchari Das and Dr. Randy Gomez. Four presenters shared their work followed by a panel discussion with the keynote speakers as well as Dr. Bill Smart. Throughout the workshop, we asked participants to write down questions on *post-it notes* for future discussion which were explored in an interactive Q&A session with the keynote speakers, Dr. Smart and Dr. Šabanović. Lastly, we broke into three groups, each focusing on a specific context, namely working with older adults in the home, working with older adults in clinical spaces, and working with children.

A. Keynotes

Our workshop features keynotes from Dr. Randy Gomez, the chief research scientists at Honda Research Institute Japan, and Dr. Sanchari Das, an assistant professor at George Mason University. Dr. Gomez discussed robots as embodied and encouraging mediators, expressing how the formation of relationships with robots in an increasingly cyber-physical world necessitates conversations about privacy. Namely, in order for social robots to be integrated for fostering well-being, they must satisfy Maslow's hierarchy of needs including safety and privacy. To iterate the use of robots in the real world, he featured the social robot Haru developed by Honda Research Institute Japan [15]. For example, he mentioned a pilot carried out in a pediatric oncological ward of a hospital where Haru serves as a social mediator for children in the hospital. He also described Haru as a social mediator across countries to foster cross-cultural communication and appreciation [14]. The talk emphasized the need to interface between law-makers and developers, highlighting also that regulation for AI lacks specific stipulations on robots and children.

Dr. Das's past work focused on user evaluations of cybersecurity solutions for smart IoT devices and interactive technologies such as social robots. In her talk she highlighted that communication about privacy risk is either ambient or users need to take intentional actions to secure their privacy, but the process for securing privacy is not always transparent or well communicated. She gave an overview of some of the multifactor authentication options and some of the perceptions and challenges for user adoption [8]. Other user evaluations highlight frustration in the risk benefit trade-offs and a lack of inclusivity. For example, physical two-factor identification keys, may not promote inclusivity given they pose elevated risk for getting lost or present users with fine motor skills greater challenges [6], [7]. Overall, she underscored the need for comprehensive and user-centered security standards for social robots in public spaces [24].

B. Contributions

Across four presentations there was a shared context of working with older adults. Two contributions described outcomes of the development and evaluation of the Interactive Robot for Ikigai Support (I.R.I.S.). Hsu and colleagues presented qualitative user evaluations of privacy and explored what privacy meant to older adults. Swaminathan and colleagues discussed a "dynamic consent mechanism" to navigate the balance between collecting enough data to personalize a robot's interactions with the risk of secure data storage and access. Xi and colleagues presented the early stages of co-designing an access control-based mechanism that can prevent robots from disclosing older adults' private information to other people. Grabler and colleagues presented their work designing an LLM based, human-in-the-loop system which could align with contextually relevant scenarios for omitting irrelevant information from data collection. Access to participant contributions can be found on the workshop's website[1].

Of the themes that were discussed, the talks considered how to utilize AI for better safeguarding older adults across different contexts, assessing the role of trust and comfort in the dynamic. Another big theme was the foundations of contextual integrity, recognizing how different scenarios demand dynamic and tailored solutions.

C. Panel Discussion

The panel generally emphasized the importance of how the framing of the robot, such as its goals or it's level of agency, affects privacy perceptions with further differences between the realities of privacy and security and a user's perceptions of privacy with the robot. The mismatch in differing goals between industry partners, users, and the scientific community was also discussed with an open question of 'who owns the collected data' as well as recognizing the challenges of explainability and transparency in the wake of black box models. Other questions posed and discussed during the panel will be discussed in Figure 1.

D. Interactive Sessions

Participants organized into three groups to discuss the contexts which influence privacy in multi-dimensional, context-dependent HRI. Namely, they focused either on robots interacting with children and teenagers in home, on classroom settings, or on robots as assistant technology for older adults.

Two groups focused on older adults: one on residential care and the other on assisted living or hospital care. In their discussion, they named a stakeholder network including older adults, family members, visitors/bystanders, repair people, clinicians, caregivers, neighbors, and the robot company/contractors. For the hospital setting, there were additional stakeholders identified such as doctors, legal guardians, and other patients.

In identifying relevant data, the group identified health data, personality, personal stories, emotional states, routines, relationships, physical household, longitudinal information,

[1]https://sites.google.com/view/privacyawarehri24/participant-contributions

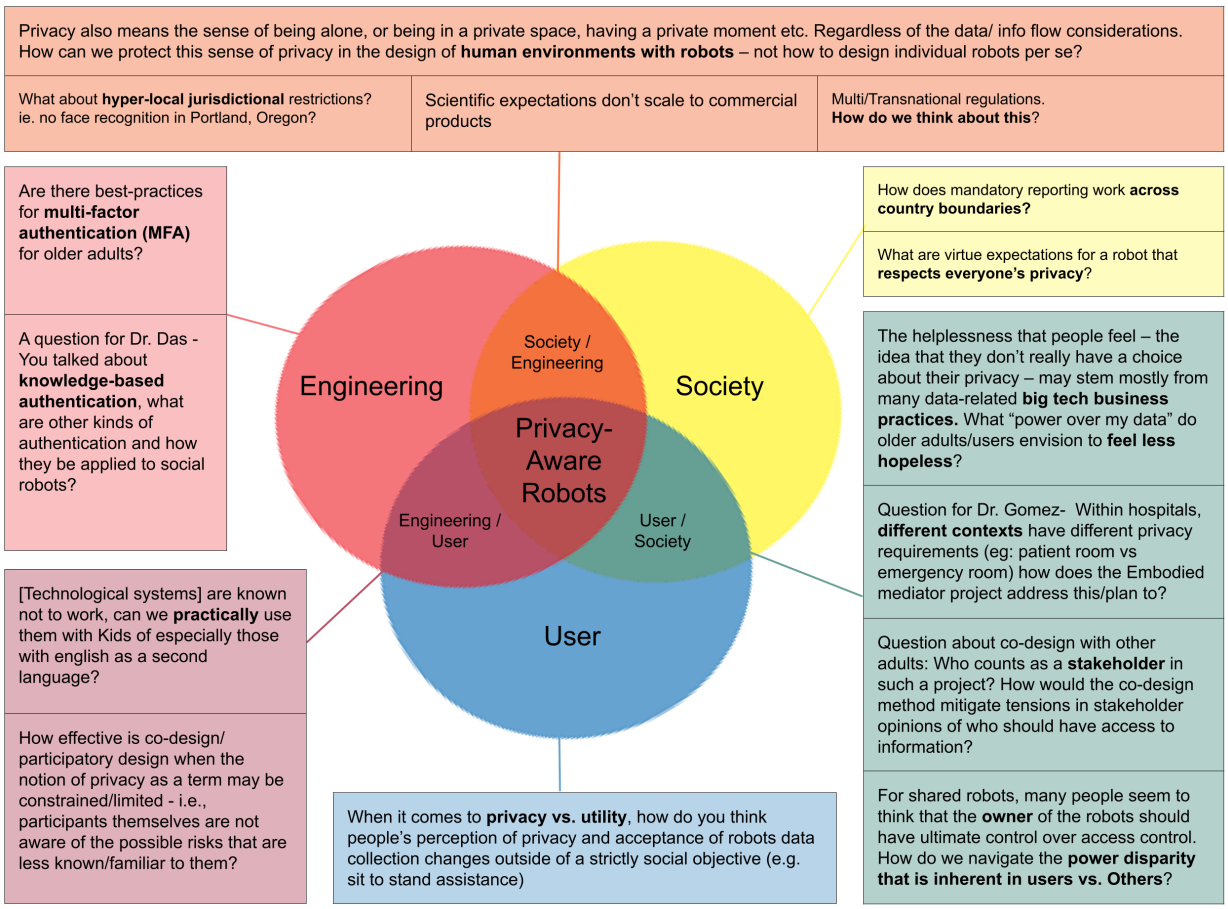

Fig. 1. Venn-diagram of workshop discussion topics and questions at the intersections of User, Society, and Engineering.

and the person's physical boundaries. The group discussing the hospital setting further considered medical data, collected and processed audio/video of conversations, behaviors or routines, and tracking personal objects.

The group discussing children considered youth under 12 years old (children) separately from youth 13-18 years old (teens). For younger children, they identified stakeholders as parents/guardians, teachers, 'imaginary peers' and friends/peers. For teens, they additionally considered college or school staff and emphasized friends in their network.

Settings where child-robot interactions may take place included school, social media/'online', the home or a safe place where they have valuable things. Kinds of information included location, photos, friendship/relationship status, and the computer's ability to recognize individuals. They also noted the potential indifference youth have towards potential threats that are unknown or they are unaware of. Additionally, they touched on the trade-offs between a youth receiving some sort of compensation or reward for information sharing and the risk of compromising their data.

III. Mapping Discussion

We conducted a reflexive thematic analysis of the 17 written questions and comments collected from participants throughout the workshop with an exploratory approach to axial coding, taking particular note of the semantic, latent, relativist, constructionist elements of the data [4]. After two rounds of reorganization and coding with the first three authors, we recognized the strength of explicitly visualizing the relationship of the comments and questions to our initial three themes of the workshop as a Venn-diagram displayed in Figure 1.

Many of the comments addressed overlapping themes, which in existing privacy research those intersections are frequently overlooked. In the overlap area between **engineering and user**, we categorized comments referring to methods and concepts for involving end-users in the privacy engineering process. This includes references to the role of end-user evaluation in testing and enhancing the real-world effectiveness of privacy implementations. The intersection of **user and society** encompasses comments about the robot as an entity within a social setting or community. This includes the potential tension between primary users and third-party stakeholders, such as citizens affected within a broader societal context. Several comments addressed the challenges within the overlap

of **engineering and society**, in designing and deploying robots that comply with various territorial privacy regulations, such as requirements for key components like facial recognition systems. Through this analysis, we identified research themes that described these overlapping fields as discuss them below.

IV. Thematic Takeaways

A. Theme 1: Real-world Effectiveness of Robot Privacy Implementations (Engineering + User)

Within this theme is the consideration of: the effectiveness of common privacy practices when applied to a social robot; the emphasis for solutions tailored to specific groups; and, the recognition of limited risk awareness among end-users. Prior research highlights a significant gap between the theoretical rigor of privacy system implementations and their real-world effectiveness [11], [31].

An example for a common shortfall in current privacy practices are lengthy consent forms and privacy policies, since they are rarely read or fully understood by consumers, undermining the principle of informed and meaningful consent [29]. One possible approach involves adapting best practices from other fields, such as cyber-security and the use of multi-factor authentication or physical security keys.

In her talk, Dr. Das highlighted some of these challenges, recognizing how multi-factor authentication procedures, while effective, are often perceived as complex and burdensome [33]. In this, effectiveness is not solely a matter of technical implementation; human factors tailored to specific user groups play a critical role.

While the challenges of effectiveness are known, limited research has been dedicated to integrating privacy engineering with user evaluation tailored specifically to the context of social robots. This gap is particularly critical, as little is known about how a robot's physical presence and interaction modalities influence users' risk awareness and their willingness to manage personal data proactively.

B. Theme 2: Contextual Stakeholder Awareness and Involvement (User + Society)

Across contexts, robots interact with people in various roles, each with distinct responsibilities and varying levels of authority. Additionally, some stakeholders are not direct users of the robots but are affected by their presence in their daily duties. This is exacerbated in cases of power imbalances between users, owners of the robots, bystanders, and the robot itself, namely with respect to who has the ability to access and control collected data. The added level of afforded agency assumed by a robot influences the interpersonal privacy between users their network [18]. Deciding the robot's role then becomes a communal and societal challenge.

Another large takeaway is the importance of studying user perceptions and involving the community in the development of privacy-sensitive design. Using co-design to design robots with stakeholders can lead to value sensitive design which can further build trust and mutual understanding between researchers and the community [40] and make space for the dynamic privacy concerns and the robot's unique utility in their space. Co-design is also an appropriate method to better learn about the perceptions and expectations for robots held by the general public [36] or vulnerable populations, such as older adults [25], [28], [16], children [22], [17], [2], and teens [3], [1]. Using co-design with these groups allows researchers to learn how different members of society envision robots within their spaces and how societal changes over time have influenced their perceptions and expectations. Future research should continue to explore how to generalize results from co-design studies surrounding fundamental rights such as privacy to the system and society levels.

C. Theme 3: Design for Regulatory Plurality (Society + Engineering)

As discussed, the nature of data protection and privacy are complicated by significantly different regulations across the world [27]. Deploying a product or service in a specific territory often requires adjustments at multiple levels. Transnational transfers of personal data remain a persistent legal challenge, even though relatively stable mechanisms, such as those governing transfers between the EU and the US, are in place [37]. While the General Data Protection Regulation (GDPR) in Europe casts a wide net, it still leaves legal uncertainty for data collection with social robots [12].

Furthermore, different rationalities are prioritized by regulators, engineers, industry, and users which complicate privacy in HRI [20]. For developers creating robots for diverse markets, the key decision lies between adopting a minimal "one-size-fits-all" implementation or pursuing a modular approach, either of which may take too broad or too narrow an approach for generalized privacy concerns.

With the rise of AI, regulatory efforts have accelerated (e.g., the EU AI Act [38]; US efforts[2]). This is particularly relevant for AI technologies used in everyday robotics, such as large language models (LLMs), emotional sensing, and biometric identification, which are under critical review. With their respective dangers, it becomes more integral to find general principles for broad applications of AI which can be agreed upon at the national and international levels [35].

In recognizing the inter-disciplinary dimensions and questions tied to privacy, we emphasize the need to host more spaces for academics, industry professionals, and politicians to consider the best ways to align creativity and potential with reasonable expectations with responsibility.

V. Conclusion

We hope this workshop and the discussions it inspired continue to push privacy research at the intersectional and multi-disciplinary facets of the field. Namely, we encourage future work which addresses the effectiveness of privacy implementations, the use of co-design with target communities, and regulatory frameworks that extend across jurisdictions.

[2]https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-united-states

References

[1] Alves-Oliveira, P., Björling, E.A., Wiesmann, P., Dwikat, H., Bhatia, S., Mihata, K., Cakmak, M.: Robots for connection: A co-design study with adolescents. In: 2022 31st IEEE International Conference on Robot and Human Interactive Communication (RO-MAN). pp. 578–583. IEEE (2022)

[2] Arnold, L., Lee, K.J., Yip, J.C.: Co-designing with children: An approach to social robot design. ACM Human-Robot Interaction (HRI) (2016)

[3] Björling, E.A., Rose, E.: Participatory research principles in human-centered design: engaging teens in the co-design of a social robot. Multimodal Technologies and Interaction **3**(1), 8 (2019)

[4] Braun, V., Clarke, V.: Thematic analysis: a practical guide (2021)

[5] Calo, M.R.: Robots and privacy. Robot ethics: The ethical and social implications of robotics p. 187 (2011)

[6] Das, S., Kim, A., Jelen, B., Streiff, J., Camp, L.J., Huber, L.: Towards implementing inclusive authentication technologies for older adults. Who Are You (2019)

[7] Das, S., Kim, A., Jelen, B., Streiff, J., Camp, L.J., Huber, L.: Why don't older adults adopt two-factor authentication? In: Proceedings of the 2020 SIGCHI Workshop on Designing Interactions for the Ageing Populations-Addressing Global Challenges (2020)

[8] Das, S., Wang, B., Kim, A., Camp, L.J.: Mfa is a necessary chore!: Exploring user mental models of multi-factor authentication technologies. In: HICSS. pp. 1–10 (2020)

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

[10] Dietrich, M., Weisswange, T.: Exploring privacy implications for domestic robot mediators. In: Proceedings of the RTSS workshop at the 2022 Conference on Intelligent Robots and Systems (IROS) (2022)

[11] Feng, Y., Yao, Y., Sadeh, N.: A design space for privacy choices: Towards meaningful privacy control in the internet of things. In: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. pp. 1–16 (2021)

[12] Fosch-Villaronga, E., Lutz, C., Tamò-Larrieux, A.: Gathering expert opinions for social robots' ethical, legal, and societal concerns: Findings from four international workshops. International Journal of Social Robotics **12**(2), 441–458 (2020)

[13] GDPR: General Data Protection Regulation (5 2018), https://gdpr.eu/ [Accessed May 31, 2023]

[14] Gomez, R., Szapiro, D., Cooper, S., Bougria, N., Pérez, G., Nichols, E., Giménez-Figueroa, J., Perez-Moleron, J.M., Peavy, M., Serrano, D., et al.: Design of embodied mediator haru for remote cross cultural communication. In: 2024 IEEE International Conference on Robotics and Automation (ICRA). pp. 5505–5511. IEEE (2024)

[15] Gomez, R., Szapiro, D., Galindo, K., Nakamura, K.: Haru: Hardware design of an experimental tabletop robot assistant. In: Proceedings of the 2018 ACM/IEEE international conference on human-robot interaction. pp. 233–240 (2018)

[16] Hsu, L.J., Kamino, W., Khoo, W., Tsui, K., Crandall, D., Šabanović, S.: Working together toward ikigai: Co-designing robots that can help us achieve meaning and purpose in life. XRDS: Crossroads, The ACM Magazine for Students **30**(1), 38–45 (2023)

[17] Levinson, L., Gomez, R., Šabanović, S.: Bow ties & colorful eyes: Centering youth designs of social robots. In: 2024 33rd IEEE International Conference on Robot and Human Interactive Communication (ROMAN). pp. 1667–1674. IEEE (2024)

[18] Levinson, L., McKinney, J., Nippert-Eng, C., Gomez, R., Šabanović, S.: Our business, not the robot's: family conversations about privacy with social robots in the home. Frontiers in Robotics and AI **11**, 1331347 (2024)

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

[20] Lutz, C., Tamò, A.: Robocode-ethicists: Privacy-friendly robots, an ethical responsibility of engineers? In: Proceedings of the ACM Web Science Conference. WebSci '15, Association for Computing Machinery, New York, NY, USA (2015). https://doi.org/10.1145/2786451.2786465, https://doi.org/10.1145/2786451.2786465

[21] Lutz, C., Tamó-Larrieux, A.: The robot privacy paradox: Understanding how privacy concerns shape intentions to use social robots. Human-Machine Communication **1**, 87–111 (2020)

[22] Mott, T., Bejarano, A., Williams, T.: Robot co-design can help us engage child stakeholders in ethical reflection. In: 2022 17th ACM/IEEE International Conference on Human-Robot Interaction (HRI). pp. 14–23. IEEE (2022)

[23] Nissenbaum, H.: Privacy in context. Stanford University Press (2009)

[24] Oruma, S.O., Ayele, Y.Z., Sechi, F., Rødsethol, H.: Security aspects of social robots in public spaces: a systematic mapping study. Sensors **23**(19), 8056 (2023)

[25] Ostrowski, A.K., Breazeal, C., Park, H.W.: Long-term co-design guidelines: empowering older adults as co-designers of social robots. In: 2021 30th IEEE International Conference on Robot & Human Interactive Communication (RO-MAN). pp. 1165–1172. IEEE (2021)

[26] Petronio, S.: Boundaries of privacy: Dialectics of disclosure. Suny Press (2002)

[27] Prasanna, S., Lavanya, P.: Navigating the maze: Understanding key data privacy and security laws worldwide. Access Here-https://scholar. google. com/scholar (2023)

[28] Rebola, C.B., Ramirez-Loaiza, S.: Co-designing technologies for well being: a robot companion for older adults. In: Advances in Information and Communication: Proceedings of the 2021 Future of Information and Communication Conference (FICC), Volume 2. pp. 871–882. Springer (2021)

[29] Reidenberg, J.R., Russell, N.C., Callen, A.J., Qasir, S., Norton, T.B.: Privacy harms and the effectiveness of the notice and choice framework. Isjlp **11**, 485 (2015)

[30] Rueben, M., Aroyo, A.M., Lutz, C., Schmölz, J., Van Cleynenbreugel, P., Corti, A., Agrawal, S., Smart, W.D.: Themes and research directions in privacy-sensitive robotics. In: 2018 IEEE workshop on advanced robotics and its social impacts (ARSO). pp. 77–84 (2018)

[31] Schaub, F., Balebako, R., Durity, A.L., Cranor, L.F.: A design space for effective privacy notices. In: Eleventh symposium on usable privacy and security (SOUPS 2015). pp. 1–17 (2015)

[32] Sebo, S., Stoll, B., Scassellati, B., Jung, M.F.: Robots in groups and teams: A literature review. Proc. ACM Hum.-Comput. Interact. **4**(CSCW2) (oct 2020), https://doi.org/10.1145/3415247

[33] Shagufta Baseer, S., Charumuthi, K.S.: Multi-factor authentication: A user experience study. International Journal of Scientific Research in Engineering and Management **8**, 1–5 (2024)

[34] Tavani, H.T.: Informational privacy: Concepts, theories, and controversies. The handbook of information and computer ethics pp. 131–164 (2008)

[35] Thimm, C., Thimm-Braun, L.: Policies, regulation and legal perspectives on social robots. De Gruyter Handbook of Robots in Society and Culture. De Gruyter (2024/i. pr.)

[36] Tian, L., Carreno-Medrano, P., Sumartojo, S., Mintrom, M., Coronado, E., Venture, G., Kulić, D.: User expectations of robots in public spaces: A co-design methodology. In: Social Robotics: 12th International Conference, ICSR 2020, Golden, CO, USA, November 14–18, 2020, Proceedings 12. pp. 259–270. Springer (2020)

[37] Tracol, X.: "schrems ii": The return of the privacy shield. Computer Law & Security Review **39**, 105484 (2020)

[38] Union, E.: Artificial intelligence act (2024)

[39] Van Den Hoven, J.: Information Technology, Privacy, and the Protection of Personal Data, p. 301–321. Cambridge Studies in Philosophy and Public Policy, Cambridge University Press (2008). https://doi.org/10.1017/CBO9780511498725.016

[40] Van Wynsberghe, A.: Designing robots for care: Care centered value-sensitive design. In: Machine ethics and robot ethics, pp. 185–211. Routledge (2020)

[41] Westin, A.F.: Privacy and freedom. Washington and Lee Law Review **25**(1), 166 (1968)