A Qualitative Observational Video-Based Study on Perceived Privacy in Social Robots' Based on Robots Appearances

Diana S. Lindblom, *Member IEEE*, Marieke van Otterdijk, and Jim Torresen, Senior *Member, IEEE*

***Abstract*— Privacy has recently got attention, especially since the introduction of the General Data Protection Regulation (GDPR) in Europe, the new Artificial Intelligence Act (AIA) and the new Machinery Regulation. Privacy can be defined as someone's right to keep personal matters, including personal life, personal information, or relationships, to themselves. A social robot's appearance (=the combination of embodiment and motion) may contribute to how human users perceive them, including how these robots are perceived in relation to privacy. If these robots are part of certain services such as home- or healthcare, these may also have consequences on how these services are perceived. This study aims at showcasing the users' perception of privacy based on the perceived robot's appearance. Three social robots were chosen for this purpose: PLEO (with a zoomorphic appearance), Pepper (with a child-like anthropomorphic appearance), and TIAGo (with a mechanical and asymmetrical appearance). The data was collected through an in-lab observational video-based study from 50 participants with very limited- or no experience with robots. Our findings show that PLEO was perceived as preserving most of the users' privacy, while Pepper was perceived as more privacy-invasive than PLEO but less than TIAGo. TIAGo was perceived as hard to interpret in terms of privacy. Our findings also point out that designing robots with a cute appearance, such as PLEO, may contribute to participants trusting the robot more and thus being willing to share their data. The paper provides a list of characteristics that participants associated with a social robot as preserving or not their privacy. Further, the paper discusses the appearance of these social robots in terms of "cuteness" as a dark pattern in the design of social robots that may lead to data myopia, but also the possible consequences this may have, for vulnerable users, while trying to design more inclusive robots.**

I. Introduction

During the next few years, social robots are predicted to be extensively used for home- and healthcare, as well as consumer products in therapy, rehabilitation, or as companion robots [1], [2], [3]. Social robots used in private environments may however pose privacy concerns or risks. At the same time, their appearances, which we defined here as the combination of the social robot embodiment and motion, can affect users' perceptions of privacy. If these robots are used, for example, in homecare settings, during rehabilitation, or therapy, users' perceptions of privacy may affect how they perceive other services as well (e.g., homecare service). Furthermore, if privacy issues arise when these robots are used as consumer products, they may also negatively impact the consumer experience.

The aim of this study was to explore people's perceptions of social robots with different appearances in relation to privacy. The paper's objective is to showcase the users' perception of privacy based on different social robots' appearances (= the combination of embodiment and motion). Thus, the research question addressed is: *How do people with limited or no experience with robots perceive social robots in terms of privacy based on their appearance (= embodiment and motion)?* Three robots were chosen for this purpose: a humanoid robot (Pepper), a social and assistive robot with a mechanical and asymmetrical appearance (TIAGo), and a zoomorphic robot (PLEO) (Fig 1.).

Figure 1: Illustration of the social robots included in the study: Pepper, TIAGo, and PLEO (from left to right)

A. Background

Privacy has recently gotten attention, especially since the introduction of the General Data Protection Regulation (GDPR) in Europe [4], the new Artificial Intelligence Act (AIA) [5], and the New Machinery Regulation [6]. Privacy can be defined as someone's right to keep personal matters, including personal life, personal information, or relationships, to themselves [7]. In Human-Robot Interaction (HRI), when social robots are used in the home- and healthcare, therapy sessions, in rehabilitation, or as consumer products, the users are often concerned with their privacy due to the robot's equipment (e.g., sensors, cameras, microphones) [8]. Concerns are related to what kind of data is collected and whether the data is sent over the Internet to other services or stakeholders to be processed through Machine Learning algorithms with the aim of improving future algorithms or models [8].

Several studies point out that privacy in HRI is a central aspect to be addressed [9], [10], [11]. The perception of privacy related to the use of social robots may affect how a service is perceived. It is, therefore, important to understand what people with limited or no experience with robots think about the privacy of robots as they may become potential future users of these technologies. This group of people are

*Research supported by Norwegian Research Council.

D.S.L Author is with the University of Oslo, Department of Informatics (IFI), Robotics and Intelligent Systems Research Group (ROBIN), Oslo, Norway, 0373 Oslo. (corresponding author: 0047 968 743 45; e-mail: dianasa@ ifi.uio.no).

M.v.O. Author is with the University of Oslo, IFI, ROBIN, and with RITMO Center of Excellence, Oslo, Norway. (e-mail: marivano@ifi.uio.no).

J. T. Author is with University of Oslo, IFI, ROBIN, and with RITMO Center of Excellence, Oslo, Norway. (e-mail: jimtoer@ifi.uio.no).

also less biased towards the use of social robots in different settings since their experiences with robots are limited. In addition, they may shed light on a larger societal issue: such as how users with limited or no experience with robots may trust social robots in terms of privacy more than those with robot literacy. It is expected that social robots will be extensively used as not only welfare technologies for the aging population in the future [12], but also as consumer products (e.g., as toys, home appliances, robot companions, etc.). However, privacy still remains an issue, "in particular when potentially vulnerable persons interact with robots"[9], [11], [12]. Hence, we wished to investigate how potential future users of these robots perceive these robots in relation to privacy based on the robots' appearances. Next, we introduce the theoretical framework of this paper.

II. Theoretical Framework: On privacy and the "Cute" Appearance Of Social Robots As A Dark Pattern

A social robot is characterized as an intelligent hub hidden behind a cute appearance. Studies argue that there is a growing trend toward such robots [13]. Lovot, Jibo, Cozmo by Anki, Honda's 3E, and Buddy by Blue Frog are examples of robots with such characteristics [14]. Cuteness in social robots reflects a sense of robot powerlessness, but at the same time, it reflects that they are exceptionally powerful [14]. Cuteness, as a design feature, creates an ideal environment for the creation of social and emotional intimacy between the human user and the robot by creating a positive affective bond between the subject (the human) and the object (the robot). Meanwhile, studies recognize that roboticists who create cute robots acknowledge these reasons themselves: they would like the robots to look like infants, and users would feel nurtured and protected by the robots, thus creating emotional bonds with them [14].

However, social robots' cuteness may deceive users when it comes to their privacy. Users may feel tempted to exchange their own data for short-term positive feelings of companionship when cute social robots appeal to their emotional feelings [14]. This issue is defined as a "dark pattern" [14]. Harry Brignull [15] introduced the concept, which is derived from the Software Engineering concept of "design patterns." This concept abstracts problems and solutions from specific use cases so that they can be applied to similar problems. In the same way, "dark patterns" are used in technology but designed to manipulate, trick, or deceive. Dark patterns are derived from persuasive design, which uses data to create designs that appeal to human emotions through the design of digital technology, such as social robots. Interaction design literature has been mainly focused on screen-based digital interactions when it comes to "dark patterns.". Recently, research also revealed that social robots are currently designed according to these dark patterns. For instance, the *cuteness* of social robots is a "dark pattern" [14]. Cute social robots may deprive users of some level of agency at the interaction level. At the same time, cute social robots create emotional responses in their interaction with humans, which may lead to "data myopia." Data myopia is defined as: "Because individual experience does not always feel unsafe, users are viscerally disengaged from the seemingly abstract dangers of data collection and aggregation, even if they know such risks exist. Our lack of felt connection to the aggregation of our everyday data, and our resulting data myopia, influence our broader attitudes toward information privacy and the appropriate flows of our personal information at a societal level." [16] (p. 21). Previous studies argue that we are more likely to enter into data-sharing agreements with social robots when we do not feel unsafe, such as when interacting with cute robots. In addition, [14] suggests dark patterns are used in technology design to give the illusion of user sovereignty. By doing this, users are given the impression that they are in control not just of their actions but also of the technology. Through gamification or other features that reward users for using technology, dark patterns can also promote addictive or compulsive behaviors. These mechanisms, as short-term gains, often outweigh the users' long-term decisions or actions. Additionally, these dark patterns are designed to exploit the users' data by appealing to their emotions and causing "data myopia." Even if these design decisions are initially made with good intentions (e.g., appealing design), they can still result in undesirable outcomes (e.g., collecting more data than is necessary about the user). Next, we present our data collection and analysis.

III. Method

There are two ways of collecting data about how users perceive privacy in relation to the appearance of social robots [17]. One can ask the users directly what they think about such a product or have direct access to a user's emotions – data that can be used to understand how they feel about a product. The former can be done through interviews or surveys, while the latter can be directly captured using eye tracking and biological signals [17]. This study was conducted as an observational study, in the university's pupillometry and eye-tracking lab, through a survey. In the study, the participants were tasked with observing three different types of robots expressing various movements in nine-second videos that included all their body parts (e.g., head, torso, arms, and legs - if any). These videos were recordings of real robots, namely PLEO (= a robot dinosaur with a zoomorphic appearance), Pepper (= a humanoid robot with a child appearance), and TIAGo (= a robot with a mechanical and asymmetrical appearance), as shown in Fig 1. These robots were mainly selected based on the representation of their embodiments (zoomorphic vs. anthropomorphic vs. mechanical and asymmetrical appearance). Other reasons for including these robots were their pre-programmed expressive behavior and similar expressive features, such as a head and limbs, but also due to their availability. Video recordings of these robots were used, as opposed to images, since we could showcase various movements in these videos. Although images may have allowed us to use a higher number of robots, images can only express the embodiments of the robots and not their motions. Thus, images are rather limited, and therefore short videos were used. The video recordings of these robots were made against a neutral background. Furthermore, the robots were filmed from three different angles, as suggested by Laeng & Rouw [18]. These angles are front, side, and ¾-angle, were selected to limit that amount of familiarization. In total, eighteen unique videos were shown in randomized order. The study was first piloted with six participants. The

duration of the experiment was 30-45 minutes. After observing each of the videos with the robots, the participants were asked to complete the survey questions. This paper presents in detail the qualitative findings from the study.

The participants were recruited in March 2022 through social media platforms and poster promotion of the study. The inclusion criteria for the study were: 1) the ability to read and write in English and b) very limited experience or no prior experience in interacting with social robots. Based on these criteria, we recruited 50 participants: 14 males with a mean age of 28.4 (SD = 6.4) and 36 females with a mean age of 25.2 (SD = 3.49). All the participants gave their informed consent to take part in the study and could withdraw from it, at any time, without giving any explanation and without any consequences for them. All participants were rewarded with a gift card of 10 EUR upon completing this survey. The study was conducted according to the ethical guidelines from the Ethical Center for Research Data (NSD) (Ref. Nr: 863869). The data was stored on the Service for Sensitive Data (TSD), at the University of Oslo, Norway.

The data presented in this paper were gathered using a survey with open- and closed-ended questions in order to understand how different types of robots and their behavior (motion) and appearance regarding privacy are perceived after seeing each of the provided short videos of robots. Participants were asked to rate the perceived privacy of the robots on a scale of 1 (= "I think that the robot does not respect my privacy at all, based on its appearance and motion") to 7 (= "I think that the robot respects very much the privacy, based on its appearance and motion") and motivate their answers. Lastly, participants were asked to describe what it would mean for them that a robot respects privacy and which features of a robot contribute to this phenomenon. The data was analyzed based on G. Walsham's (2006) method [19]. Based on the participants' answers, the data was sorted into themes and issues focusing on the idea of privacy as the guiding principle for the analysis. The categories for each of these were re-visited a couple of times while looking for eventual contradictions in the data. Excel and MS Word were used to document during the whole process. In the end, the themes were sorted. These themes guided the writing of the findings, as presented in the next section.

IV. FINDINGS

In general, the majority of the participants associated some characteristics, such as robot capabilities, robot appearance, or design of the robots, with privacy. However, a few (n=7) of the participants did not specifically think about eventual privacy issues when interacting with a robot. They clearly indicated that they could not relate to the robots' privacy aspects. In general, we asked the participants to rate perceived privacy in relation to each of the robots, on a scale from 1 (= "I think that the robot does not respect my privacy at all, based on its appearance and motion") to 7 (= "I think that the robot respects very much the privacy, based on its appearance and motion"). The standard deviation was *SD*=1.62, while the mean = 3.92. This means that the majority of the participants rated perceived privacy between 2.3-5.54. This means that the participants had some concerns about their own privacy when using social robots, while others did not, although they had very limited experience with social robots. Table 1 shows a summary of the characteristics associated with robot privacy based on the users' perception.

A. Robot appearance and privacy: participants think that humanoid robots respect less human privacy than robotic toys

Regarding the robot's appearance and whether these robots respect people's privacy, the opinions among the participants varied. PLEO, for instance, was viewed as familiar, as a toy, or a pet, and the participants did not consider it as privacy-intrusive, as some of the participants indicated: *"I considered the Dino robot to have as use-case just being a toy, so I am not worried about it.*", "*Maybe the dino respects my privacy a little more than the humanoid because I wouldn't expect a dino to be interested in my private stuff at all*.", "*Because they look familiar, and I assume that they would respect my privacy as an animal,*" "*I believe I found the Dinosaur robot was respecting my privacy and beliefs because he was just acting like a dog.*", "*The dinosaur seemed like a pet to me, and I feel like pets do not really invade our privacy. They might just need attention, and that is it.*" In contrast, two of the participants experienced that PLEO was respecting their privacy less because the robot appeared as curios and as an animal: "*felt a bit like an animal, and animals usually don't respect privacy like they don't seem to understand that you need space.*" Another point indicated by one of the participants was that the robot is equipped with "*fewer screens or camera-like eyes*," and therefore, it appeared that it would protect more privacy. Regarding Pepper, some of the participants (14%) associated its humanoid appearance and the presence of a screen on its chest with perceiving it as a privacy-invasive robot. However, the robot seemed to be able to move on its own and could move its head away: this feature made the robot also as being perceived as possibly respecting more the privacy of the users, as one participant pointed out: "*It had the possibility to look away*." TIAGo, on the other hand, was perceived as a machine that would not understand privacy or commands. One participant clearly indicated that: "*The one-armed robot and the human-like robot both seemed like they had no sense of privacy or awareness for that matter*." Another participant specified that TIAGo was "*hard to read*," and therefore, it was perceived as not respecting its privacy. Thus, the legibility of the robot was important in the users' perception of privacy.

While some of the participants clearly referred to some specific robots, when reflecting on privacy, 38% of the participants talked about privacy and robots in general. Only 22% of the participants stated that the robots did not feel intrusive or that all robots would respect their privacy. Here are a few examples: "*All of the robots seem reliable to protect my privacy*.", "*I did not find any of them not respecting my privacy*," "*These robots didn't feel intrusive at all*," "*I have no particular feeling of respecting my privacy from these robots*.", "*All of them respect my privacy*." In contrast, only 16% of participants were quite concerned about their privacy when it comes to social robots. Some of the concerns enumerated included: the companies behind the

robots, various data types collected by the robot, or that the robots do not understand social cues and, therefore, they are not able to respect one's privacy. Finally, just 12% of the participants seemed to be aware of the connection between privacy and the robot design. In general, the participants put the responsibility of a privacy-respecting robot on the designer, but also on whom has access to the robot or the data collected by the robot. Other participants would argue that they would feel more comfortable regarding their privacy if the robot would not be connected to any network, while others would argue that robots can respect one's privacy if they are well-programmed.

TABLE I. CHARACTERISTICS ASSOCIATED WITH PERCEIVED PRIVACY IN SOCIAL ROBOTS – ACCORDING TO THE PARTICIPANTS

Robot Charcateristics	***Does not give feelings of privacy***	***Gives feelings of privacy***
Appearance	Machine-like appearance Non-friendly appearance	A toy appearance Familiar look Pet Look Friendly Appearance
Behavior	The robot does not behave according to social norms Does not respect spatial and/or emotional privacy Impolite Aggressive behavior Too bold behavior Loud behavior Invasive behavior	Being able to move its head away Pre-programmed to respect one's privacy The robot behaves according to social norms Respecting spatial and/or emotional privacy Polite Non-aggressive behavior Humble behavior Quit behavior Respectful behavior It does not "listen" all the time
Control	Hard to read the intentions of the robot Depends on the company behind the robot Being connected to a network A third party having access to users' data Does not follow the users' commands	Easy to understand the robot's intentions Depends on the company behind the robot Not being connected to a network A third party not having access to the users' data Follows the users' commands User's control over what type of data is collected User's control over how the data is processed The user is able to turn off the robot Explicit consent is given by the user The user is able to switch ON/OFF the microphone, speakers, etc. It inspires trust
Functionalities and Capabilities	Presence of screens and eyes Does not understand social cues	Move away by itself Fewer screens and/or eyes Understand social cues Warning or indicating when data is recorded
Robot Charcateristics	***Does not give feelings of privacy***	***Gives feelings of privacy***
	Do not warn or indicate when data is recorded Audio/video recordings without consent The robot does not understand social norms	Audio/video recording with the consent It can turn OFF by itself The robot understands social norms

B. Privacy in relation to social robots – as defined by the participants

We asked the participants how they would define privacy in relation to social robots. In general, the participants indicated one or several characteristics of a robot that are to be perceived as respecting or not their privacy. The participants associated the privacy of robots with the following parameters (listed from the maximum to the minimum number of appearances): 1) capabilities of the robot and 2) robot design and appearance. Only two participants could not relate the concept of privacy to social robots, as they stated: "*I can't really tell how a robot can respect my privacy or not.", "I have never been in a situation where a robot would disrespect my privacy. In fact, I think the intention is the most part of the issue when someone violates our privacy. Since the robots can not have intentions, I do not think they can neither respect nor disrespect our privacy*." Privacy respecting robots in relation to the 1) capabilities of the robot was defined by the participants in terms of the following four characteristics: whether the robot follows the commands from the human (36%), whether the robot discloses personal data (22%), whether it understands social norms (18%), and how it behaves (12%). It seems that for many of the participants (36%) was important that the robot followed their commands and that they could feel that they were in control. The participants pointed clearly out that they wished they were in control of the robot. They also indicated that the robot should look away when it is told to do so, without gathering data about them if the user did not wish that. Similarly, the participants explained that they wished to have control over what kind of data is collected and also to be able to turn the robot off. Similarly, three participants specifically indicated that they wished to give explicit consent if data were collected by the robot. Further, the participants wished to have control over the processing of their data. Along the same lines, many participants (22%) associated the idea of privacy in HRI with their personal data not being disclosed to a third party. The participants also explained that the robot should warn them when it records data about them, but it should also not save their data. One of the participants expressed in an explicit way that s/he wanted to know the type of data the robot was recording in the case of a recording. Similarly, one participant reported feelings of discomfort if s/he were to be audio or video recorded, especially if s/he was not aware of that. Amongst other robot capabilities expressed by the participants in relation to their perception of privacy in social robots was that it was important for the participants

that the robot understands (and acts according to) social norms (18%). This includes that the robot should understand social norms regarding its behavior related to privacy but also that the robot respects when a person does not wish to interact with it. The participants clearly expressed, in some cases, that a robot should respect the privacy of others exactly as a human does: "*It's important, just like humans should respect each other's privacy*." Furthermore, a few participants (12%) pointed out that the behavior of the robot can be associated with (dis)respecting their privacy. Specifically, for these participants, it was important that the robot shows respect for privacy in terms of spatial privacy, but also emotional privacy. At the same time, one participant expressed that the robot should behave in a polite way, not being too loud or too invasive, whereas another participant expressed that the robot should not behave aggressively, be too bold, or be too engaged while also keeping a physical distance.

Privacy respecting robots in terms of the 2) robot design and appearance was defined by the participants based on the following characteristics: whether the robot was designed according to privacy by design principles (20%), how the robot appears (12%), and whether the robot gives feelings of safety or not based on its appearance (2%). 20% of the participants associated privacy in social robots with privacy by design, such as the participants expected the robot to have built-in features that make the robot respect one's privacy. Amongst these features, there were named: the possibility to switch ON/OFF the microphone, camera, or sensors, that the robot informs when it is recording, that it can move away by itself with the purpose of not recording data, that it can completely turn off by itself, and that does not "*listen*" all the time, even when it seems to be off. In addition, the participants pointed out that the robot software should be built in accordance with GDPR and not collect data without consent. Moreover, it also seemed that the appearance of the robot seemed to be of high importance for at least some of the participants (12%). They interpret it as a robot respecting their privacy if it appears as friendly, keeps a distance when needed, if it looks familiar, and shows gestures of politeness. In that way, it seems that the participants would feel that the robot is more trustworthy, thus also respecting their privacy.

V. Discussion: On Perceived Privacy Based on Robot Appearance

In this study, we have addressed the research question: *How do people with limited or no experience with robots perceive social robots in terms of privacy based on their appearance (= embodiment and motion)?* We have answered the research question through a qualitative observational video-based study, that included a survey, where we looked at the appearance of three social robots, namely PLEO (with a zoomorphic appearance), Pepper (= with a child-like anthropomorphic appearance) and TIAGo (with a mechanical and asymmetrical appearance), in relation to participants' perceived privacy. 50 participants took part in the study. Our findings show that PLEO was not considered privacy-invasive at all because it has a familiar appearance as a toy but also as a pet. The participants expected that the robot would behave similarly to a pet in terms of privacy. Pepper, on the other hand, was considered more privacy-invasive than PLEO but less privacy-invasive than TIAGo. The reasons given were that the robot was equipped with a screen, potentially also with microphones and sensors, but also that it was able to turn its head away. TIAGo, however, was perceived as a machine-like robot that was not aware of privacy aspects and whose social cues were hard to read.

It seems that PLEO, due to its toy appearance, was trusted more than a machine-like robot such as TIAGo. The research shows that the cute appearance of robots is used as a dark design pattern, often capitalizing on the users' informational privacy [14] and leading to data myopia in the user. For instance, such an example is the Japanese Lovot robot, where design is used "to usher new technologies of surveillance into the domestic spaces and quotidian lives of older adults" [20]. Moreover, research also shows that users tend to disclose personal or private aspects to robots that look cute or have a friendly or pleasant appearance, social robots being a challenge to informational-, physical-, psychological-, and social privacy due to both their capabilities to create social bonding with the users, but also due to their autonomy [21]. In this sense, there is a risk that vulnerable users, the elderly, children, or care receivers, become even more vulnerable when they are given these kinds of robots to interact with without being aware of their privacy-invasiveness. While it seems that users have sovereignty over the robots that look cute, appearing as the users are the ones who are empowered, actually, the software and the company behind the robot are the ones who truly have sovereignty [14]. Nevertheless, [14] contends that users may become data myopic because of the cuteness of robots. It is dishonest to design a robot that is cute but has the intention of leading the user into data myopia [14]. Users' (information) privacy and data protection are directly affected by this type of design. Further, when asked how the participants would define privacy in relation to robots, we noticed that some of the participants were not aware of potential privacy issues. Others would instead associate privacy issues with the robot's capabilities to look away, to follow commands, and social norms. Similarly, the participants wished to have control over their personal data, to know how the data is processed, and when the robot is recording audio or video data about them. Social cues, e.g., the robot being polite, not too bold, too loud, or too invasive, were associated with increased privacy by the participants. At the same time, the participants wished that the robot had built-in features that preserved their privacy. A lack of transparency in the design of these social robots may prevent users from understanding what data is collected about them [22]. Thus, while models of social robots aim to empower vulnerable groups, designers and roboticists risk of creating dark patterns in their designs that lead to data myopia.

VI. Concluding Remarks

In this paper, we investigated how people with limited or no experience with robots perceive social robots in terms of privacy. A video survey was conducted using three robots with different appearances (PLEO, Pepper, and TIAGo). We asked the participants questions about their perceived privacy based on the appearance of these robots. The study shows that the participants perceived the three robots

differently in terms of privacy: PLEO was perceived as preserving the most the users' privacy; Pepper was perceived as more privacy-invasive than PLEO, but less than TIAGo; TIAGo was perceived as hard to interpret in terms of privacy. Moreover, the study also shows that social robots that appear they respect users' privacy do not necessarily respect the privacy of the user. The paper also provides a compiled list of concrete characteristics associated with perceived privacy in social robots based on the 50 participants' answers. Thus, we can conclude that the robots' appearance (embodiment and motion) affects how the robot is perceived [22] and consequently may also affect how services that they are part of are perceived. This may have serious consequences if the social robot is part of, for instance, home- or healthcare services. However, the study is limited to only three robots, and 50 participants, with limited or no experience with robots, in the Norwegian context. Thus, the generalizability of the study should be treated as such. All in all, it seems that there is a need for further studies regarding privacy in social robots [21], [23].

ACKNOWLEDGMENT

This work is partially supported by The Research Council of Norway as part of the Vulnerability in Robot Society (VIROS) project (grant agreement 288285) and the Predictive and Intuitive Robot Companion (PIRC) project (grant agreement 312333), along with RITMO Centre of Excellence, at University of Oslo (Project No. 262762). Special thanks to the participants, to the University of Eindhoven for borrowing to us the Pepper robot, and to Prof. Bruno Laeng for allowing the use of his lab for this data collection.

REFERENCES

[1] S. Bedaf, G. J. Gelderblom, and L. de Witte, "Overview and Categorization of Robots Supporting Independent Living of Elderly People: What Activities Do They Support and How Far Have They Developed," *Assistive Technology*, vol. 27, no. 2, pp. 88–100, Apr. 2015, doi: 10.1080/10400435.2014.978916.

[2] R. Bemelmans, G. J. Gelderblom, P. Jonker, and L. de Witte, "The Potential of Socially Assistive Robotics in Care for Elderly, a Systematic Review," in *Human-Robot Personal Relationships*, M. H. Lamers and F. J. Verbeek, Eds., in Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Berlin, Heidelberg: Springer, 2011, pp. 83–89. doi: 10.1007/978-3-642-19385-9_11.

[3] R. Bemelmans, G. J. Gelderblom, P. Jonker, and L. de Witte, "Socially assistive robots in elderly care: a systematic review into effects and effectiveness," *J Am Med Dir Assoc*, vol. 13, no. 2, pp. 114-120.e1, Feb. 2012, doi: 10.1016/j.jamda.2010.10.002.

[4] European Union, "General Data Protection Regulation (GDPR) Compliance Guidelines," GDPR.eu. Accessed: Jan. 19, 2021. [Online]. Available: https://gdpr.eu/

[5] European Commision, "Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) | Shaping Europe's digital future." Accessed: Apr. 30, 2021. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence

[6] European Commision, "Proposal for a Regulation of the European Parliament and of the Council on machinery products." Accessed: Apr. 23, 2021. [Online]. Available: https://ec.europa.eu/docsroom/documents/45508

[7] "Privacy," *Cambridge English Dictionary*. 2023. Accessed: Mar. 01, 2023. [Online]. Available: https://dictionary.cambridge.org/dictionary/english/privacy

[8] T. Schulz, J. Herstad, and H. Holone, "Privacy at Home: An Inquiry into Sensors and Robots for the Stay at Home Elderly," in *Human Aspects of IT for the Aged Population. Applications in Health, Assistance, and Entertainment*, J. Zhou and G. Salvendy, Eds., in Lect. Notes in Comp. Sci. Cham: Springer International Publishing, 2018, pp. 377–394. doi: 10.1007/978-3-319-92037-5_28.

[9] D. Saplacan and J. Tørresen, "Robots as Welfare Technologies to Reduce Falls Amongst Older Adults: An Explorative Study from Norway," in *Human Aspects of IT for the Aged Population. Technology in Everyday Living*, Q. Gao and J. Zhou, Eds., in Lecture Notes in Computer Science. Cham: Springer International Publishing, 2022, pp. 88–106. doi: 10.1007/978-3-031-05654-3_6.

[10] J. Torresen, "A Review of Future and Ethical Perspectives of Robotics and AI," *Front. Robot. AI*, vol. 4, 2018, doi: 10.3389/frobt.2017.00075.

[11] F. M. Noori, Z. Uddin, and J. Torresen, "Robot-Care for the Older People: Ethically Justified or Not?," in *2019 Joint IEEE 9th International Conference on Development and Learning and Epigenetic Robotics (ICDL-EpiRob)*, Aug. 2019, pp. 43–47. doi: 10.1109/DEVLRN.2019.8850706.

[12] L. Bodenhagen, S.-D. Suvei, W. K. Juel, E. Brander, and N. Krüger, "Robot technology for future welfare: meeting upcoming societal challenges – an outlook with offset in the development in Scandinavia," *Health Technol.*, vol. 9, no. 3, pp. 197–218, May 2019, doi: 10.1007/s12553-019-00302-x.

[13] U. Pagallo, "The Impact of Domestic Robots on Privacy and Data Protection, and the Troubles with Legal Regulation by Design," in *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, S. Gutwirth, R. Leenes, and P. De Hert, Eds., in Law, Governance and Technology Series. , Dordrecht: Springer Netherlands, 2016, pp. 387–410. doi: 10.1007/978-94-017-7376-8_14.

[14] C. Lacey and C. Caudwell, "Cuteness as a 'dark pattern' in home robots," in *Proceedings of the 14th ACM/IEEE International Conference on Human-Robot Interaction*, in HRI '19. Daegu, Republic of Korea: IEEE Press, Jan. 2020, pp. 374–381.

[15] H. Brignull, "Deceptive patterns - user interfaces crafted to trick you." Accessed: Mar. 28, 2023. [Online]. Available: https://www.deceptive.design/

[16] L. Stark, "The emotional context of information privacy," *The Information Society*, vol. 32, no. 1, pp. 14–27, Jan. 2016, doi: 10.1080/01972243.2015.1107167.

[17] T. Laohakangvalvit, T. Achalakul, and M. Ohkura, "Kawaii feeling estimation by product attributes and biological signals," in *Proceedings of the 18th ACM International Conference on Multimodal Interaction*, in ICMI '16. New York, NY, USA: Association for Computing Machinery, Oct. 2016, pp. 563–566. doi: 10.1145/2993148.2997621.

[18] B. Laeng and R. Rouw, "Canonical views of faces and the cerebral hemispheres," *Laterality*, vol. 6, no. 3, pp. 193–224, Jul. 2001, doi: 10.1080/713754410.

[19] G. Walsham, "Doing interpretive research," *Eur J Inf Syst*, vol. 15, no. 3, pp. 320–330, Jun. 2006, doi: 10.1057/palgrave.ejis.3000589.

[20] C. Lafontaine, "Towards Lively Surveillance? The Domestication of Companion Robots," in *Human Aspects of IT for the Aged Population. Healthy and Active Aging*, Q. Gao and J. Zhou, Eds., in Lecture Notes in Computer Science. Cham: Springer International Publishing, 2020, pp. 486–496. doi: 10.1007/978-3-030-50249-2_35.

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

[22] M. K. Lee, K. P. Tang, J. Forlizzi, and S. Kiesler, "Understanding users' perception of privacy in human-robot interaction," in *Proceedings of the 6th international conference on Human-robot interaction*, in HRI '11. New York, NY, USA: Association for Computing Machinery, Mar. 2011, pp. 181–182. doi: 10.1145/1957656.1957721.

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