International Journal of Social Robotics (2023) 15:1487–1505
https://doi.org/10.1007/s12369-023-01043-8

Never Trust Anything That Can Think for Itself, if You Can't Control Its Privacy Settings: The Influence of a Robot's Privacy Settings on Users' Attitudes and Willingness to Self-disclose

Julia G. Stapels[1] · **Angelika Penner**[1] · **Niels Diekmann**[2] · **Friederike Eyssel**[1]

Accepted: 9 August 2023 / Published online: 22 September 2023

Abstract
When encountering social robots, potential users are often facing a dilemma between privacy and utility. That is, high utility often comes at the cost of lenient privacy settings, allowing the robot to store personal data and to connect to the internet permanently, which brings in associated data security risks. However, to date, it still remains unclear how this dilemma affects attitudes and behavioral intentions towards the respective robot. To shed light on the influence of a social robot's privacy settings on robot-related attitudes and behavioral intentions, we conducted two online experiments with a total sample of $N = 320$ German university students. We hypothesized that strict privacy settings compared to lenient privacy settings of a social robot would result in more favorable attitudes and behavioral intentions towards the robot in Experiment 1. For Experiment 2, we expected more favorable attitudes and behavioral intentions for choosing independently the robot's privacy settings in comparison to evaluating preset privacy settings. However, those two manipulations seemed to influence attitudes towards the robot in diverging domains: While strict privacy settings increased trust, decreased subjective ambivalence and increased the willingness to self-disclose compared to lenient privacy settings, the choice of privacy settings seemed to primarily impact robot likeability, contact intentions and the depth of potential self-disclosure. Strict compared to lenient privacy settings might reduce the risk associated with robot contact and thereby also reduce risk-related attitudes and increase trust-dependent behavioral intentions. However, if allowed to choose, people make the robot 'their own', through making a privacy-utility tradeoff. This tradeoff is likely a compromise between full privacy and full utility and thus does not reduce risks of robot-contact as much as strict privacy settings do. Future experiments should replicate these results using real-life human robot interaction and different scenarios to further investigate the psychological mechanisms causing such divergences.

Keywords Social robot · Data protection · Privacy · Self-disclosure · Attitudes towards robots · Ambivalence

1 Introduction

Many roboticists claim that social robots will soon be present in private households to assist, to provide entertainment or companionship [1–3]. Social robots can be defined as robots which "exhibit personality and communicate with [human beings] using high-level dialogue and natural cues" [1, p. 441]. In its function as a robotic companion for humans, a social robot is expected to engage in human interactions in a socially acceptable way. Several robot capabilities are needed to meet user expectations. This includes, for instance, the perception and recognition of the user, the ability to analyze facial expression, the tone of voice, gestures and patterns of movement. To achieve such perception and understanding of human expression and behavior, a social robot is bound to be equipped with adequate technology, such as cameras

Julia G. Stapels and Angelika Penner Shared co-first authorship.

✉ Angelika Penner
angelika.penner@uni-bielefeld.de

Julia G. Stapels
julia.stapels@tu-dortmund.de

Niels Diekmann
niels.diekmann@fh-bielefeld.de

Friederike Eyssel
friederike.eyssel@uni-bielefeld.de

[1] Department of Psychology, Center for Cognitive Interaction Technology, Bielefeld University, Bielefeld, Germany

[2] Bielefeld University of Applied Sciences, Bielefeld, Germany

or sensors. This might include facial and voice recognition and room detection sensors. For the purpose of human interactions, a social robot ought to have sufficient computer and memory capacity at its disposal [4]. To ensure timely processing of substantial data such as verbal information, facial expression and body language, a social robot might be required to collect and store large amounts of data. As a mean to obtain such capacity, it might be necessary to connect social robots with an external storage center and with the internet.

Effectively, a social robot monitors the user in their utmost private environment. From this, privacy-related issues emerge. For instance, depending on the specific design or purpose, a social robot collects, processes, and stores personal information, which might be considered private or sensitive [5]. Moreover, social robots could be abused for unauthorized access to personal information. A variety of social robots are capable to roam around autonomously. Their ability to perceive their environment is therefore not restricted to one specific place. Thus, social robots store vast amounts of private and sensitive information which could be conveyed to third parties [6]. These potential risks to user privacy raise social, ethical, and legal questions which will be addressed in this paper.

In an ever-increasing digitalized world, privacy is an ubiquitous concern [e.g., 7]: To illustrate, users receive notifications on web pages which emphasize the high *value* or *respect* placed on user privacy prior to asking for permission to use tracking devices (cookies). However, it is still not possible to reach absolute data privacy, so that individuals have to compromise between privacy issues and making use of the benefits of information sharing [7]. Whereas the importance of privacy concerns is out of question, there is no consensus upon the definition and classification of privacy and it varies broadly [8]. For instance, Burgoon [8] reviews the literature on privacy definitions and differentiates four dimensions of privacy: Physical privacy, social privacy, psychological privacy, and—ultimately—informational privacy. The dimension of physical privacy refers to being unheard and unseen [8]. Social privacy entails feeling safe in a social setting while being isolated from outsiders [8]. Obtaining social privacy implies to be able to create closeness between some individuals, while simultaneously excluding others or maintaining a social distance to them. Psychological privacy describes the ability to think freely, to be in control of the own cognitive processes and to control whom to confide one's own thoughts [8]. Ultimately, informational privacy goes beyond psychological privacy regarding data control, as it also relates to data which individuals can collect through observation or data which are stored through technology use without the user's knowledge. Psychological privacy, in particular, is associated with self-disclosure [8], as psychological privacy entails to determine towards whom people want to self-disclose and under which circumstances. Thus, psychological privacy might be the key aspect to investigate when linking it to the vast literature on human–robot interaction (HRI). Moreover, informational privacy is important within the HRI context because of the data storage capacity required to keep a robot up and running. However, all these aforementioned dimensions of privacy have to be taken into account in order to design a privacy-compliant social robot that shall not merely be tolerated, but accepted by potential end users. According to the privacy calculus model [7], potential users estimate costs of information sharing towards technologies, which are mostly privacy-related, and benefits of information sharing which can be manifold but should be worth the privacy loss. Previous research has shown that privacy concerns are an important part of potential users' attitudes towards robots [9, 10]. One way to account for such privacy concerns and to enhance psychological privacy is to design novel technologies, such as social robots, in a way that incorporates users' concerns and wishes regarding their privacy and gives them agency over their shared data [11]. In the current work, we investigated the psychological consequences of such privacy settings—which may be determined either by choice or by default. To sum up, the many facets of privacy should be considered in the development of social robots and in the context of HRI. However, besides psychological aspects of privacy, legal aspects and circumstances need to be considered for the development of a privacy-respecting robot for real-life contexts.

1.1 The Law of Privacy and Data Protection

The human desire for privacy is reflected in the law of privacy and data protection. A multitude of laws has been enacted in many countries to protect their respective citizens from undue intrusion of their homes. Equally, laws have been introduced to protect confidentiality of mailing services, telephone service and so forth. Thus, if social robots for private home environments are being developed, the legal side of privacy and data protection should be taken into account.

The concept of a universal *right to privacy* is mostly associated with the work of Warren and Brandeis [12]. In the year 1890, these authors already alluded to the fact that indeed, mechanical devices could threaten personal rights. Things that were said in confidence could be spread broadly through such mechanical devices [12]. Therefore, they concluded that the existing legal provisions should be expanded to protect privacy in its entirety. Basically, the idea of a right to privacy lies within the traditional concept of property; the idea of individual belonging of distinct objects to one person or a group of persons and not to someone else or the commonalty whether these objects are tangible or intangible [12]. To exemplify, a secret told in the home environment with a social robot present still belongs to the individual telling

the secret and not to the social robot or the robot operator which might have access to the robot's stored data. More recent work dealing with regulations of the European Court of Human Rights and the European Court of Justice points out that looking only for privacy interference is possibly obsolete [13]. Besides protecting against privacy interference safeguarding that collected and stored data and meta-data is not used to gain control and to dominate people was put into focus [13].

Article 12 of the Universal Declaration of Human Rights (UDHR, 2015) states that "No one shall be subjected to arbitrary interference with his privacy […]" and "Everyone has the right to the protection of the law against such interference or attacks". Privacy is addressed as an enforceable right in numerous legal provisions (such as Art. 8 European Convention on Human Rights, 2021). With regard to the former example, a social robot ideally possesses protection mechanisms against hacking and the robot operator ideally protects any data they might have access to through social robots.

Within the 1970s, some European countries enacted data protection laws [14]. With the enactment of the General Data Protection Regulation (GDPR, 2016), the European Union has inaugurated a new trend on the protection of privacy and personal data worldwide [15]. The increase of data protection is related to developments in informational technology, such as the appearance of the internet, the arrival of wireless communication devices and data-mining software [7, 14]. Such increased possibilities to access data raise a need for more sophisticated data protection laws. This is especially relevant for social robots which operate in the private home of individuals, retrieve and store possibly sensible data, have access to the internet and, unlike for example smartphones, might move independently in the home environment. In such cases, the processing of personal data shall only be performed for specified purposes and "on the basis of the consent of the person concerned or some other legitimate basis laid down by law" (Art. 8 (2) Charter of Fundamental Rights of the European Union (CFR, 2000)). The individual is entitled by law to demand information about data processing concerning him or her, and to demand correction. Thus, when companies collect and store personal data of a robot's user they should only do so with explicit consent for specified purposes, e.g., to ensure robot functionality, and be able to provide information about and change user information.

Whereas a robot operator would not be allowed to share personal data of their robots' users, the individual is free to disseminate their own personal data. The disclosure of personal data, and thereby, a loss of privacy is often a necessity for conversation, transactions and general human interaction [e.g., 16, 17]. This will likely be the case for social robots, too. To give an example, a user would need to disclose music preferences in order to let the robot play music that the user likes when instructed to start music. In interpersonal interactions, an individual constantly weights costs and benefits of sharing information [18]. Sharing information with a robot entails benefits which might be worth the costs, e.g., privacy loss. Giving users control over their potential privacy loss might help them to balance those benefits and costs. The concept of *privacy by design* aims at maintaining such individual control. The general idea of privacy by design is to focus the conditions of data processing on the intentions and needs of the individual. As already argued, the development of social robots might benefit from the idea of privacy by design.

1.2 Privacy by Design and Social Robots

By designing social robots, developers have to balance the need for user privacy and robot performance. For instance, a household robot that is free to roam the user's apartment might be swifter to interact and assist in daily routines. However, the user might feel hassled and would like to restrict the robotic presence to certain spaces. For instance, users might forbid a robot to enter the bathroom because people are more privacy-sensitive in their bathroom or their bedroom compared to their living room or kitchen [19]. Moreover, if a social robot is using its visual recordings permanently, it can observe its environment and react to changes, such as the reappearance of its user or the user's non-verbal behavior. However, the user might feel unduly monitored and therefore restricted in his or her liberties. To protect privacy, the notion of privacy by design postulates that technologies should safeguard privacy by privacy-friendly default settings, beginning from the design stage of a new technology [20]. One way to account for such fine-tuned robot management is through technologies such as apps, where access rights can flexibly be granted or restricted [5]. Besides users' privacy concerns, another challenge for HRI regarding privacy is to ensure that other stakeholders of social robots, e.g., the robot company and the developers, do implement privacy-friendly settings. In fact, even if privacy by design could be implemented in social robots, possibly business and state interests stand in the way of a widespread implementation [21]. To exemplify, a robot company might want to collect user data to gain a better understanding of user needs or for other reasons and a state could want to get access to private data of users to prevent or uncover criminal acts. Therefore, not only technical solutions are needed, but also strategies are required to get stakeholders of data collecting and storing technologies on board to build privacy-friendly technologies, e.g., social robots [11]. Results on the influence of privacy settings on user attitudes and behavioral intentions might contribute to the attitude formation of these stakeholders.

Evidently, the potential risk of privacy loss increases if personal data are not only collected, but stored [22]. Any data

storage entails the risk of misuse, alteration and accidental or intentional disclosure. However, a social robot that is capable of evaluating past experiences based on stored data might be more advanced in social interactions and therefore might provide extended services to the user. This is particularly true if a social robot even has the ability to access data collected by other robots [23].

Finally, an even greater infringement upon privacy could potentially arise from a social robot that is temporarily or permanently connected with the internet. Personal information such as images or whereabouts shared via internet are available to the outside world and could be evaluated, disseminated or published. Potentially, the internet connection could be used for spying or unauthorized seizure of the robot. However, the ability of a social robot to interact properly with its user might heavily depend upon the level of computing capacity which is potentially greater with an internet connection. An internet connection might be needed even more so, when the social robot is supposed to entertain conversation with its human user in a natural acting fashion. Evidently, cloud-based services provide greater computing speed and capacity that is needed to enable naturally sounding responses within conversations than a local data processor [6]. Thus, the conflict of a social robot's utility and usability and a user's privacy is ought to be taken into account in the process of developing and designing social robots. Other technologies have already been developed that adhere to privacy by design. For instance, a speech assistant that provided nutrient information to elderly users was evaluated positively in a study, especially highlighting the possibility of not sharing voice data and operating offline [24]. Such possibilities might become even more relevant when video data and personal data about people's everyday lives are registered by the device. Social robots may only reach the goal of being a companion in everyday life if the individual balance of privacy and disclosure can be ascertained for each user.

2 Related Work

2.1 Privacy Concerns in Social Robotics

Privacy is not only relevant in legal aspects concerning the use of social robots but influences psychological aspects of HRI as well. Attitudes towards robots are often described as neutral [e.g., 25, 26]. However, recent research has shown that users are in fact highly conflicted in their attitudes towards robots, resulting in negative affect and an inability to commit to a positive or negative attitude [27]. One reason for this ambivalence concerning social robots may be privacy concerns. Users have various concerns regarding the privacy of their data when interacting with robots, e.g., concerning the access storage of their private information [e.g., 10; for an overview, see 28]. This is also reflected in psychological research: In a recent study a social robot provided positive psychology interventions which increased users' psychological well-being [29]. In this study, many users felt threatened concerning their privacy through the robot's technological features and behavior. Those privacy concerns of potential users should be addressed in the development of social robots to improve the willingness to interact with them.

2.2 Psychological Factors in Attitudes Towards Robots

When people interact with their environment, important social needs emerge and call for satisfaction, e.g., the need for competence, autonomy, and relatedness, which entail the desire to experience oneself as competent, able to make autonomous decisions, and to be connected to others [30]. Social robots have the potential to address such needs: Ideally, they are easy to handle interaction partners that support users in their autonomous decisions. However, previous research has likewise shown that users feel threatened by robot autonomy and the associated anticipated lack of controllability [31]. Thus, it appears plausible that robots with strict privacy settings evoke more positive and less negative attitudes compared to robots with lenient privacy settings because with strict privacy settings users stay more in control over their private information. However, the extent to which a social robot features lenient privacy correlates with its utility [19, 32]. That is, a social robot with lenient privacy settings might provide more functions compared to a social robot with strict privacy settings: For instance, a robot that stores and connects lots of data is better at recognizing faces and giving suggestions based on the user's behavior compared to a robot with restrictive settings. To gain unlimited functionality potentially goes at the cost of a user's privacy. Therefore, strict privacy settings might not necessarily lead to unequivocally positive attitudes. That is, users might feel ambivalent regarding the tradeoff between functionality and privacy (for an overview, see [33]). Specifically, the way the VIVA robot that was used in the present research was designed, stricter settings, such as local data storage and offline functionality, would have led to a loss of knowledge-related features [5, 34]; however it is possible that robots that are currently being developed retain full functionality while offline. To resolve such privacy-related attitudinal conflict some psychological mechanisms might be promising candidates.

One of the psychological mechanisms that influence attitudes towards robots concerns the issue whether the user is allowed to select the preferred privacy settings. Relatedly, previous research has shown that being able to choose features of the robot—in this case—the robots design, had a positive impact on users' attitudes towards robots [35, 36]. This is in line with the well-established 'Ikea'- or 'I designed

it myself' effect that has been studied in social psychology: Research on this phenomenon has shown that users' attitudes towards an attitude object improve, e.g., they perceive more value in the object [37], feelings of competence [38] and autonomy increase [39] when users are allowed to participate in the making of a product. The effect is especially strong when users may make a broad array of selections according to their preferences while at the same time having to put in little effort. Clearly, participating in the design process of a product contributes positively to users' attitudes towards the product [40]. Previous research has introduced the potential of an app controlling certain aspects of a social robot's privacy-related behavior in order to mitigate users' concerns [5]. Thereby, users were able to balance their individual need for privacy with their individual need for robot utility. Through the app it was even possible to adapt this balance to specific situations and contexts. To illustrate, users might choose to set the strictest possible privacy settings for their social robot during a private gathering in their home to protect not only their own privacy, but also the privacy of the guests. This is done because highly personal information may be shared by attendees of such gathering.

Another psychological mechanism involved in the realm of privacy during HRI is related to attitudinal ambivalence. This is the simultaneous existence of positive and negative evaluations that likely results in inner conflicts [41]. Recent work has demonstrated that attitudinal ambivalence is relevant in the context of social robots and social robots have been shown to evoke high levels of attitudinal ambivalence [27]. That is, potential users apparently feel torn between hopes for a high usability and usefulness of robots and likewise experience fears of being isolated, of being physically threatened by robots or think that such technology would invade their personal space [10]. Thus, being able to control features and functions of a robot, such as its privacy settings, might serve as a coping mechanism to attenuate the conflict induced by ambivalence.

In the current line of research, we investigated whether attitudes towards robots improve, e.g., become less ambivalent, the stricter the privacy settings. Moreover, we investigate whether attitudes towards robots improve when the users actively take part in privacy-related product decisions. In addition to attitudes towards robots, we also look at a specific behavioral intention, i.e., the willingness to self-disclose, which is likely influenced by privacy settings of a social robot.

2.3 Privacy and Self-Disclosure

Another aspect which is probably in a mutual relationship with not only attitudes towards robots, but also with privacy settings, is a user's self-disclosure towards a social robot. Self-disclosure can be defined as "what individuals verbally reveal about themselves to others" [42, p. 1]. Self-disclosure varies in depth—meaning the level of intimacy of shared information—and breadth—the extent to which personal information is shared [16]. According to social penetration theory [16], individuals disclose more about themselves when new relationships develop and become gradually more personal. Indeed, self-disclosure and liking are positively correlated [43]. Moreover, privacy settings are associated with the willingness to self-disclose. To exemplify, the influence of privacy settings on participants' attitudes has been previously investigated in the domain of online self-disclosure of personal information [44]. According to these results, privacy and trust are important determinants of self-disclosure. Thus, a social robot's privacy settings might be important for the willingness to self-disclose towards it.

Self-disclosure is known to have several positive functions [e.g., 18], and even self-disclosing towards robots might be beneficial for users [e.g., 45]. At the same time, self-disclosing towards a robot poses a privacy risk [e.g., 8]. Self-disclosure is determined by various psychological motives that are associated with social reward: Social approval, intimacy, relief of distress, social control, and identity clarification [18]. Similar psychological rewards of self-disclosure might occur when disclosing towards an artificial agent like a chatbot or a robot. To illustrate, self-disclosure in a chat with a chatbot or a person result in similar positive emotional, relational and psychological outcomes [46]. The same might be true for robots, e.g., related to relief of distress through self-disclosure to a robot [45], even though this still has to be investigated more thoroughly. In one case, people who experienced strong negative affect through a negative mood induction benefitted more from talking to a robot compared to just writing their thoughts and feelings down [47]. This result indicates that self-disclosure towards robots also serves the relief of distress motive. Another recent study showed that people who felt more lonely during the COVID-19 pandemic compared to before pandemic were more willing to self-disclose towards a social robot [48]. This result could be interpreted in a way that people might want to self-disclose towards a robot to feel more connected. In case social connectedness with humans is under threat, the motivation to self-disclose towards robots might increase. Disclosing personal information towards social robots might be also beneficial, not only for psychological outcomes for users, but also for a robot's function: A robot could adapt to users' needs and habits based on their self-disclosures [e.g., 49]. For example, to be deemed an acceptable robot companion, the robot ideally should know which interaction styles a given user prefers, e.g., the frequency the robot should ask whether the user wants the robot's service, and which special needs the user might have, e.g., being informed on the weather every morning, and adapt accordingly [50]. To enable such user-centered adaptation, users indeed need to

reveal at least some kind of personal information to their companion robot to ensure a smooth interaction. Overall, it needs to be investigated more thoroughly if findings of human–human interaction (HHI) literature on self-disclosure reasons also apply for HRI. However, the results of some studies [48] already point out that there might be parallels between HHI and HRI, as supported by the media equation theory [51].

Besides the reviewed benefits of self-disclosure in HRI, self-disclosure is also associated with various risks: The disclosure decision model proposes a number of risks associated with self-disclosure, namely social rejection, betrayal, and causing discomfort to the recipient of the disclosure [18]. Betrayal is related to privacy, as it concerns the subjective fear that previously disclosed information could be passed on to third parties without permission of the discloser [17]. Thus, loss of privacy is a risk of self-disclosure [52]. This risk of self-disclosure is especially relevant for disclosures high in intimacy [18]. This is due to the fact that sharing intimate information leaves an individual more vulnerable than sharing non-intimate information. Through self-disclosure of intimate information, a recipient of self-disclosure receives power over a discloser because the recipient could develop an unfavorable opinion about the discloser based on the disclosure and since the recipient could pass the disclosed information to third parties [e.g., 17]. Thus, the discloser's privacy is at risk. The latter risk is especially important for each scenario in which the disclosed data is saved and available online, as is possible for social robots. Storing data online increases privacy risk [e.g., 22, 53]. Concerning robots, people are very aware of such privacy risks [10]: When people were asked to list negative thoughts or feelings they have when thinking about an interaction with a social robot the most frequently called aspect was privacy concerns.

If an individual discloses information towards a social robot or in proximity to it, the subjective risk of self-disclosure may not only depend on the expectations on the robot itself to keep the disclosure confidential, but also on the privacy settings of the robot. As social robots need to store data about individuals to interact individually with them and many robots rely on cloud services, potential users could fear that those stored data could be stolen by others [50]. Moreover, privacy settings have an impact on the likelihood of data being stolen or misused. Thus, the more lenient privacy settings are, the more subjective risk of self-disclosure is entailed. In a practical sense, when privacy settings of a robot are lenient and thus go along with higher risks of privacy violation, individuals might be less willing to self-disclose towards it. This might also be true when the self-disclosure is directed towards a human while being in proximity to a robot: If the robot can collect and store the disclosed information, it does not matter if the robot itself is the recipient of the disclosure to entail a loss of privacy risk.

If individuals would benefit from disclosing towards a social robot but privacy concerns would prevent individuals to disclose, recommendations for privacy settings of robots for personal use could be derived. To exemplify, we might recommend users to determine high-risk situations like private gatherings where privacy settings should be particularly strict. A robot might even recognize a private gathering and then automatically set the privacy settings as strict as possible. Thereby, users might be more comfortable to use a robot in a private environment.

3 The Present Experiments

Taking into account the existing literature from law, psychology, and social robotics, it becomes evident that privacy is a serious concern in the context of using and deploying robots: People are aware of the privacy risks associated with robot usage [e.g., 10]. On the one hand, a social robot's utility relies on user data, e.g., on habits and preferences in daily life, so that a robot may adapt to its user. On the other hand, using and storing data represents a legal and practical challenge because a user's privacy needs to be protected. From a legal perspective, it is the robot developers' duty to protect a user's personal space. Furthermore, protecting privacy is of practical interest since satisfying privacy-related needs are likely to increase likeability, trust, and contact intentions, as well as the willingness to self-disclose towards a robot. In a set of two experiments, we aimed to investigate the role of privacy settings on attitudes and behavioral intentions towards robots. In Experiment 1, we manipulated privacy settings on an absolute level, namely comparing lenient and strict privacy settings. In Experiment 2, we manipulated privacy in a user-centered way, comparing self-chosen with preset privacy settings.

All experimental manipulations were implemented in the context of the newly developed social robot named VIVA (https://navelrobotics.com/viva). We conducted extensive research on the social, legal and practical aspects and implications associated with VIVA's use [e.g., 10, 27, 54, 55]. One important feature of the robot VIVA indeed is its conformity to EU privacy laws. VIVA was developed to provide utmost utility while protecting user privacy. Additionally, it features the possibility for users to control privacy-related aspects themselves. As the robot VIVA was designed to be a companion for users in their homes, it is of essence that they feel comfortable to disclose towards the robot VIVA or at least at the presence of the robot VIVA, as the robot will likely witness conversations of users with other people. In order to investigate the psychological effects of such strict privacy settings on attitudes and behavioral intentions towards the robot, we first contrasted them with more lenient privacy settings in Experiment 1.

4 Experiment 1

In Experiment 1, we manipulated whether a robot featured strict vs. lenient privacy settings. In this online experiment, one group evaluated a robot with strict privacy settings (strict privacy condition). The other group evaluated a robot with lenient privacy settings (lenient privacy condition). The preregistration can be accessed via https://aspredicted.org/fx26c.pdf. We expected that attitudes towards the robot would be more favorable in the strict privacy condition compared to the lenient privacy condition, resulting in the following hypotheses:

Hypothesis 1: Robot likeability is higher in the strict privacy condition than in the lenient privacy condition.

Hypothesis 2: Trust towards the robot is higher in the strict privacy condition than in the lenient privacy condition.

Hypothesis 3: Contact intentions towards the robot are higher in the strict privacy condition than in the lenient privacy condition.

Previous research on attitudes towards social robots has shown that a prominent feature of robot-related attitudes is ambivalence [for an overview see 56]. We expect that through attenuating one of potential users' main concerns in the use of social robots, namely privacy violations, users develop more favorable attitudes towards social robots.

Hypothesis 4: Subjective ambivalence is lower in the strict privacy condition than in the lenient privacy condition.

Hypothesis 5: Objective ambivalence is lower in the strict privacy condition than in the lenient privacy condition.

Consequently, behavioral intentions towards the robot in the form of willingness to self-disclose are expected to vary between conditions, since data security is an important factor in self-disclosure.

Hypothesis 6: (a) Depth of self-disclosure, and (b) breadth of self-disclosure are higher in the strict privacy condition than in the lenient privacy condition.

4.1 Method

4.1.1 Participants and Design

131 participants completed the online questionnaire via Qualtrics between September and December 2020. As preregistered, we excluded three participants due to not having responded meticulously, resulting in the desired sample size of 128 participants of which 33 were male, 93 female and two diverse ($M_{age} = 26.13$, $SD_{age} = 8.64$). 111 participants were students. We manipulated robot privacy via text-vignettes on two levels (strict vs. lenient).

4.1.2 Experimental Manipulation

To provide a context for the experimental manipulation, participants were presented with three possible data-related settings, ordered from strict to lenient settings (local save, upload certain data to a cloud, upload all data automatically to a cloud) and three possible connection settings (internet connection on request, temporary internet connection, permanent internet connection), respectively. For the experimental manipulation, participants were then presented with a possible configuration of VIVA's privacy settings that could be used for the market-ready robot, depending on the condition. To reflect a lenient privacy condition, the data-related settings were set to "upload all data automatically to a cloud" and the connection settings were set to "permanent internet connection". To represent the strict privacy condition, the data-related settings were, in turn, set to "local save" and the connection settings were set to "internet connection upon request". The robot's price was set as 3,000 € in both conditions, orienting on the approximate anticipated price of the robot VIVA as indicated by the project partners at the time of the experiment.

4.1.3 Measures

All variables were measured on 7-point Likert scales from 1 (not at all) to 7 (very much). Cronbach's alpha values are reported as measured in the current experiments.

Robot Likeability We assessed robot likeability with six items ($\alpha_{Exp1} = .90$, $\alpha_{Exp2} = .90$), five of which were adapted from Reysen [57] and one item was adapted from Salem et al. [58], e.g., "VIVA is friendly.".

Trust Trust towards the robot was measured with four items ($\alpha_{Exp1} = .84$, $\alpha_{Exp2} = .76$) adapted from [59], e.g., rating VIVA from "not trustworthy" to "trustworthy".

Contact Intentions We measured contact intentions towards the robots with five items ($\alpha_{Exp1} = .90$, $\alpha_{Exp2} = .88$) adapted from Eyssel and Kuchenbrandt [60], e.g., "How much would you like to meet the VIVA robot?".

Subjective Ambivalence Subjective ambivalence was assessed using the mean of three items ($\alpha_{Exp1} = .86$, $\alpha_{Exp2} = .90$) adapted from [61] i.e., "To what degree do you have mixed feelings concerning the VIVA robot?", "To what degree do you feel indecisive concerning the VIVA robot?", "To what degree do you feel conflicted concerning the VIVA robot?".

Objective Ambivalence We computed objective ambivalence with the help of two items asking for positive and

negative evaluations separately, e.g., "When you think of the positive aspects of the VIVA robot and ignore the negative aspects, how positively do you evaluate this robot?", and vice versa. We calculated a value for objective ambivalence using the Griffin formula of ambivalence: (P + N)/2 − |P − N|. High values indicate high ambivalence and low values indicate low ambivalence [62].

Self-disclosure To measure depth of self-disclosure, we asked with one item how intimate participants would let a conversation with the robot VIVA be, with an intimate conversation meaning to discuss topics which they usually address only with familiars, while a less intimate conversation means to discuss topics they would also discuss with relatively unfamiliar people. The scale measuring depth of self-disclosure ranged from 1 (not at all intimate) to 7 (very intimate). Breadth of self-disclosure was assessed with one item asking for the preferred length of conversation with the robot VIVA from 1 (as short as possible) to 7 (as long as possible).

Additional Variables As a manipulation check, we assessed participants' perceived privacy risk elicited by the robot [63] ($\alpha_{Exp1} = .92$, $\alpha_{Exp2} = .90$). For a conjoint analysis of the factors data storage, internet connection, and price for willingness to buy the robot, participants were furthermore presented with all combinations of the data-related and the connection settings and three price options (2,000 €, 3,000 €, 4,000 €), resulting in 27 combinations. To enable the conjoint analysis, participants were asked to indicate how much they would like to buy the robot for each combination. Finally, concerning dispositional variables, we assessed technology commitment [64] ($\alpha_{Exp1} = .85$, $\alpha_{Exp2} = .84$) and chronic loneliness [65] ($\alpha_{Exp1} = .85$, $\alpha_{Exp2} = .83$).

4.1.4 Procedure

After providing informed consent, participants were presented with a description and a picture of the robot VIVA. Participants were informed in a text vignette that VIVA was a social robot for the home use that was currently under development. It was described as being able to engage in simple conversations, to recognize emotions, and to react accordingly. Moreover, the text vignette stated that VIVA would be able to perceive its environment and to move around independently [see also 10]. Participants were further told that VIVA could have various data-related settings and connection settings, on which other functions, like recognizing people and enabling updates would depend. They were then presented with the experimental manipulation consisting of an introduction of all settings followed by a text-based vignette of a robot with either strict or lenient privacy settings. Participants were then asked to evaluate the presented robot.

Furthermore, participants were instructed to evaluate 27 combinations of data storage, internet connection settings, and price for the conjoint analysis. Subsequently, they were asked to choose settings for a robot themselves and evaluate their objective and subjective ambivalence again. Finally, we assessed chronic loneliness, technology commitment, demographic information, and asked whether participants had participated meticulously. Participants were thanked and debriefed.

4.2 Results

4.2.1 Main Analyses

As a manipulation check, we investigated whether perceived privacy risk was higher in the lenient privacy condition ($M = 5.08$, $SD = 1.25$) than the strict privacy condition ($M = 3.70$, $SD = 1.51$). This was indeed the case ($t(126) = 5.62$, $p < .001$, $d = 0.99$). To test Hypothesis 1 that posited higher robot likeability in the strict privacy condition compared to the lenient privacy condition, we ran a t-test. Contrary to Hypothesis 1, robot likeability was not significantly higher in the strict privacy condition ($M = 3.65$, $SD = 1.29$) compared to the lenient privacy condition ($M = 3.53$, $SD = 1.36$), $t(126) = -0.52$, $p = .301$, $d = 0.09$. However, in line with Hypothesis 2, trust towards the robots was significantly higher in the strict privacy condition ($M = 3.87$, $SD = 1.21$) than the lenient privacy condition ($M = 3.38$, $SD = 1.23$), $t(126) = -2.25$, $p = .013$, $d = 0.39$, indicating a small effect according to Cohen [66]. Furthermore, concerning Hypothesis 3, contact intentions towards the robot were not significantly higher in the strict privacy condition ($M = 3.49$, $SD = 1.39$) compared to the lenient privacy condition ($M = 3.25$, $SD = 1.56$), $t(126) = -0.93$, $p = .177$, $d = 0.16$. In accordance with Hypothesis 4, subjective ambivalence was significantly lower in the strict privacy condition ($M = 4.20$, $SD = 1.19$) compared to the lenient privacy condition ($M = 4.64$, $SD = 1.43$), $t(126) = 1.89$, $p = .030$, $d = 0.33$, indicating a small effect. This effect did not transfer to objective ambivalence: Contrary to Hypothesis 5, objective ambivalence was not significantly lower in the strict privacy condition ($M = 2.73$, $SD = 1.88$) compared to the lenient privacy condition ($M = 2.55$, $SD = 2.16$), $t(126) = -0.51$, $p = .696$, $d = 0.09$. With regards to self-disclosure, in accordance with Hypothesis 6, the willingness to self-disclose was higher in the strict privacy condition compared to the lenient privacy condition. This was the case for both depth of self-disclosure ($M_{strict\ privacy} = 3.71$, $SD_{strict\ privacy} = 1.64$; $M_{lenient\ privacy} = 2.58$, $SD_{lenient\ privacy} = 1.45$; $t(126) = -4.14$, $p < .001$, $d = 0.73$) and breadth of self-disclosure ($M_{strict\ privacy} = 3.37$, $SD_{strict\ privacy} = 1.34$; $M_{lenient\ privacy} = 2.78$, $SD_{lenient\ privacy} = 1.46$; $t(126) = -2.34$, $p = .010$, $d = 0.41$), indicating small to medium effects.

4.2.2 Exploratory Analyses

We conducted a conjoint analysis using 27 combinations of the data-related and the connection settings and three price options (2,000 €, 3,000 €, 4,000 €). Choice-based conjoint analyses can be used to investigate preferred attributes of products, and have been used to investigate the privacy-utility tradeoff concerning voice assistants [32]. For each of the 27 combinations, participants were asked how much they would like to buy the respective robot. The values that result from the analysis indicate the relative importance (r.i.) of the features for the decision making, meaning that they indicate how important a feature is for the decision making [32]. The relative importance ranges from 0 to 100% and adds up to 100%. Results showed that data-related settings had the largest impact on the user's evaluation (*r.i.* = 40.39), followed by the connection settings (*r.i.* = 33.34) and the price (*r.i.* = 26.28). For the data-related settings, the medium option (upload certain data to a cloud) was preferred. For the connection settings, also the medium option (temporary internet connection) was preferred.

After the evaluations of all combinations of settings, participants were asked to choose their preferred settings and we assessed subjective and objective ambivalence again. Subjective ambivalence was significantly higher concerning the robot with the preset privacy settings ($M = 4.42$, $SD = 1.33$) compared to the robot with the self-chosen privacy settings ($M = 3.76$, $SD = 1.33$), $t(126) = 5.86$, $p < .001$, $d = 0.50$. Also, objective ambivalence was significantly higher concerning the robot with the preset privacy settings ($M = 2.64$, $SD = 2.02$) compared to the robot with the self-chosen privacy settings ($M = 2.15$, $SD = 1.92$), $t(126) = 2.62$, $p = .005$, $d = 0.25$.

Concerning correlational analyses, we investigated correlations between all variables (see Table 1). Technology commitment correlated positively with contact intentions ($r(126) = .27$, $p = .002$) and negatively with objective ambivalence ($r(126) = -.25$, $p = .005$). That is, people with higher technology commitment seemed to be more willing to interact with a robot and experienced fewer opposing evaluations. However, there was no significant correlation between technology commitment and likeability, trust, self-disclosure and subjective ambivalence. Furthermore, loneliness correlated significantly with objective ambivalence ($r(126) = .19$, $p = .027$). This might indicate that lonely individuals experience more opposing evaluations concerning robots. Interestingly, these dispositional variables seemed to influence the objective existence of evaluations, but not the experienced conflict, namely subjective ambivalence. Interestingly, perceived privacy risk showed significant correlations with all main dependent variables. People who perceived the privacy risk as high, evaluated the robot as less likeable ($r(126) = -.30$, $p < .001$), trustworthy ($r(126) = -.49$, $p < .001$), had less contact intentions ($r(126) = -.28$, $p = .001$), experienced higher ambivalence (subjective: $r(126) = .24$, $p = .005$, objective: $r(126) = .22$, $p = .013$), and were less willing to self-disclose (depth: $r(126) = -.51$, $p < .001$, breadth $r(126) = -.34$, $p < .001$). We provide a table of all correlations with a confidence interval of 0.99 in Table 1.

4.3 Discussion

In Experiment 1, we investigated the impact of strict vs. lenient robot privacy settings on attitudes concerning the robot. To do so, we presented participants with text-based vignettes of a robot's privacy related settings and assessed robot likeability, robot-related trust, contact intentions, attitudinal ambivalence and intention to self-disclose towards the robot. In sum, not all hypotheses could be supported by empirical evidence. In line with Hypotheses 2, 4 and 6, trust, as well as depth and breadth of self-disclosure, were higher in the strict privacy condition compared to the lenient privacy condition, and subjective ambivalence was lower in the strict privacy condition compared to the lenient privacy condition. However, there was no significant difference concerning robot likeability, contact intentions, and objective ambivalence. It seems like manipulating privacy in absolute terms i.e., strict vs. lenient, especially influences trust and trust-related behavioral intentions, i.e., self-disclosure, as well as subjective ambivalence, which might also be strongly influenced by trust. It seems that these dependent variables benefit most from reduced privacy risk. In contrast, likeability, contact intentions, and objective ambivalence appear to be independent from an objective privacy risk. As stated before, not only potential users' subjective judgment of the privacy settings' rigor, but also a sense of control over privacy settings might influence our dependent variables significantly. To investigate if control over privacy settings has similar effects on attitudes and behavioral intentions as strict vs. lenient privacy settings itself, in Experiment 2, we manipulated whether the privacy settings were preset or chosen by the participants. Furthermore, to assess compensatory cognitions as a consequence of ambivalence, in Experiment 2 we also measured personal belief in a just world. Compensatory cognitions, specifically belief in a just world, have been shown to result from ambivalence as a means to cope with attitudinal conflict, even if the ambivalent attitude objects are unrelated to such compensatory cognitions [68].

5 Experiment 2

To test the idea that providing a choice to select privacy settings would have a beneficial impact on participants' attitudes towards a robot, we formulated the hypotheses in parallel to those tested in Experiment 1. The preregistration can be

Table 1 Means, standard deviations, and Pearson correlations with confidence intervals between all measures

Variable	*M*	*SD*	1	2	3	4	5	6	7	8	9
1. Privacy risk	4.40	1.55									
2. Likeability	3.59	1.32	− .30***								
			[− .49, − .08]								
3. Trust	3.62	1.24	− .49***	.51***							
			[− .65, − .30]	[.32, .66]							
4. Contact intentions	3.37	1.48	− .28**	.59***	.51***						
			[− .48, − .06]	[.42, .72]	[.32, .66]						
5. Subjective ambivalence	4.42	1.33	.24**	− .20*	− .06	− .03					
			[.02, .45]	[− .41, .03]	[− .28, .17]	[− .25, .20]					
6. Objective ambivalence	2.64	2.02	.22*	.02	− .09	− .10	.04				
			[− .01, .43]	[− .21, .24]	[− .31, .14]	[− .32, .13]	[− .19, .26]				
7. Depth of self-disclosure	3.14	1.64	− .51***	.43***	.44***	.42***	− .16	− .04			
			[− .66, − .32]	[.22, .60]	[.24, .61]	[.22, .60]	[− .37, .07]	[− .27, .19]			
8. Breadth of self-disclosure	3.07	1.43	− .34***	.39***	.46***	.50***	− .10	− .10	.60***		
			[− .53, − .13]	[.17, .56]	[.26, .62]	[.31, .66]	[− .32, .13]	[− .32, .13]	[.43, .73]		
9. Loneliness	1.86	0.70	.09	.06	− .03	.03	.04	.19*	.00	.05	
			[− .14, .31]	[− .17, .28]	[− .26, .19]	[− .20, .26]	[− .19, .26]	[− .03, .40]	[− .22, .23]	[− .18, .27]	
10. Technology commitment	4.69	1.06	− .17	.17	.03	.27**	.06	− .25**	.14	.09	− .09
			[− .38, .06]	[− .06, .38]	[− .20, .26]	[.05, .47]	[− .17, .28]	[− .45, − .02]	[− .09, .35]	[− .14, .31]	[− .31, .14]

M and *SD* are used to represent mean and standard deviation, respectively. Values in square brackets indicate the 99% confidence interval for each correlation. The confidence interval is a plausible range of population correlations that could have caused the sample correlation [67]. *indicates $p < .05$. **indicates $p < .01$. ***indicates $p < .001$

accessed via https://aspredicted.org/kr46j.pdf. We hypothesized that attitudes and behavioral intentions towards the social robot would be more favorable if the participants were able to choose the privacy settings themselves (choice condition) compared to preset privacy settings (no choice condition).

Hypothesis 1: Robot likeability is higher in the choice condition than in the no choice condition.

Hypothesis 2: Trust towards the robot is higher in the choice condition than in the no choice condition.

Hypothesis 3: Contact intentions towards the robot are higher in the choice condition than in the no choice condition.

Hypothesis 4: Subjective ambivalence is lower in the choice condition than in the no choice condition.

Hypothesis 5: Objective ambivalence is lower in the choice condition than in the no choice condition.

Hypothesis 6: (a) Depth of self-disclosure, and (b) breadth of self-disclosure are higher in the choice condition than in the no choice condition.

5.1 Method

5.1.1 Participants and Design

216 participants completed an online questionnaire via Qualtrics between April and November 2021. As preregistered, we excluded 24 participants due to not having participated meticulously, resulting in the desired sample size of 192 participants of which 60 were male, 131 female and one open declaration ($M_{age} = 26.21$, $SD_{age} = 9.09$). 150 participants were students. We manipulated robot privacy settings on two levels, giving participants the opportunity to choose the settings in one condition and providing preset settings on a medium level, which was the mostly chosen setting in Experiment 1, in the other condition (choice vs. no choice).

5.1.2 Experimental Manipulation

As in Experiment 1, participants were presented with the same possible data-related settings (i.e., local save, upload certain data to a cloud, upload all data automatically to a cloud) and connection settings (i.e., internet connection on request, temporary internet connection, permanent internet connection). For the experimental manipulation, participants were either presented with a possible configuration of VIVA's settings on a medium level with which the robot might be sold or were asked to choose the settings themselves. In the no choice condition, the data-related settings were set to a medium level as "upload certain data to a cloud" and the connection settings were set as "temporary internet connection". In the choice condition, participants could choose from the three options for data-related and connection settings, respectively. The price was again set as 3,000 € in both conditions.

5.1.3 Measures

We employed the same dependent variables as in Experiment 1, extended by the Personal Beliefs in a Just World (PBJW) questionnaire with seven items ($\alpha = .90$), e.g., "I am usually treated fairly" [69]. This variable was included to explore potential consequences of ambivalent attitudes towards robots [56]. Specifically, ambivalence may lead to compensatory cognitions, such as a higher belief in a just world after being exposed to ambivalent stimuli, even if the stimuli and beliefs are unrelated [68]. Here, we aimed to explore whether participants compensated the ambivalent attitudes evoked by the robot by showing higher perceptions of order, in this case operationalized by higher personal beliefs in a just world.

5.1.4 Procedure

After providing informed consent, participants were presented with a description and a picture of the robot VIVA. Participants were presented with all possible data-related and storage settings as in Experiment 1. This was followed by a description of a robot with medium settings (no choice condition) or the task to choose their preferred settings themselves (choice condition), depending on the experimental condition. They were then asked to evaluate the respective robot. Thereafter, we assessed PBJW, chronic loneliness, technology commitment, demographic information, and asked whether participants had participated meticulously. Finally, participants were thanked and debriefed.

5.2 Results

5.2.1 Main Analyses

On a descriptive level, participants in the choice condition seemed to choose all options concerning connection settings equally (i.e., internet connection on request (31 times), temporary internet connection (31 times), permanent internet connection (36 times)) while there might be a tendency towards the middle concerning data storage (i.e., local save (24 times), upload certain data to a cloud (62 times), upload all data automatically to a cloud (12 times)).

Again, we used t-tests to examine our hypotheses that robot likeability, trust towards the robot, contact intentions towards the robot, and willingness to self-disclose would be

higher, and ambivalence would be lower towards the robot in the choice condition compared to the no choice condition. In line with Hypothesis 1, robot likeability was significantly higher in the choice condition ($M = 3.91$, $SD = 1.33$) compared to the no choice condition ($M = 3.55$, $SD = 1.40$), $t(190) = 1.81$, $p = .036$, $d = 0.26$, indicating a small effect. However, in contrast to Hypothesis 2, trust towards the robot was not significantly higher in the choice condition ($M = 3.84$, $SD = 1.12$), compared to the no choice condition ($M = 3.88$, $SD = 1.22$), $t(190) = -0.26$, $p = .602$, $d = 0.04$. Furthermore, concerning Hypothesis 3, contact intentions towards the robot were significantly higher in the choice condition ($M = 3.79$, $SD = 1.40$) compared to the no choice condition ($M = 3.40$, $SD = 1.52$), $t(190) = 1.85$, $p = .033$, $d = 0.27$, indicating a small effect. In contrast to Hypothesis 4, subjective ambivalence was not significantly lower in the choice condition ($M = 4.30$, $SD = 1.56$) compared to the no choice condition ($M = 4.03$, $SD = 1.65$), $t(190) = 1.17$, $p = .878$, $d = 0.17$. Also, contrary to Hypothesis 5, objective ambivalence was not significantly lower in the choice condition ($M = 2.69$, $SD = 1.92$) compared to the no choice condition ($M = 2.55$, $SD = 2.00$), $t(190) = 0.48$, $p = .684$, $d = 0.07$. In accordance with Hypothesis 6, depth of self-disclosure was higher in the choice condition ($M = 3.37$, $SD = 1.46$) compared to the no choice condition ($M = 2.96$, $SD = 1.28$), $t = 2.07$, $p = .020$, $d = 0.30$, indicating a small effect. However, breadth of self-disclosure was not significantly higher in the choice condition ($M = 3.41$, $SD = 1.60$) compared to the no choice condition ($M = 3.17$, $SD = 1.64$), $t(190) = 1.02$, $p = .155$, $d = 0.15$.

5.2.2 Exploratory Analyses

For the exploratory variables, we again investigated correlations between the individual variables and the main dependent variables (see Table 2). As in Experiment 1, loneliness correlated significantly with objective ambivalence ($r(190) = .19$, $p = .008$), but not with the other variables. In Experiment 2, technology commitment correlated significantly with robot likeability ($r(190) = .27$, $p < .001$), trust ($r(190) = .16$, $p = .028$), contact intentions ($r(190) = .34$, $p < .001$), subjective ambivalence ($r(190) = -.17$, $p = .020$), and depth of self-disclosure ($r(190) = .20$, $p = .006$). Perceived privacy risk was negatively correlated with likeability ($r(190) = -.28$, $p < .001$), trust ($r(190) = -.48$, $p < .001$), contact intentions ($r(190) = -.35$, $p < .001$), breadth of self-disclosure ($r(190) = -.33$, $p < .001$) and depth of self-disclosure ($r(190) = -.46$, $p < .001$) and positively with subjective ambivalence ($r(190) = .35$, $p < .001$), similar to Experiment 1. As a new variable, we investigated belief in a just world, since previous research has shown that ambivalence induces compensatory cognitions, which can manifest in unrelated control strategies, as a higher belief in just world [68]. However, belief in a just world correlated negatively only with objective ambivalence ($r(190) = -.18$, $p = .010$) and not with subjective ambivalence.

5.3 Discussion

In Experiment 2 we investigated the influence of self-chosen vs. preset privacy settings on attitudes and behavioral intentions towards a robot. In line with our hypotheses and the "I designed it myself" effect [40], participants evaluated the robot with the settings they chose themselves as more likeable and participants reported higher contact intentions compared to the robot with preset settings. They were also willing to disclose more in-depth personal information to the robot with self-chosen privacy settings. However, attitudes and behavioral intentions were not always more favorable concerning the choice condition. There were no significant differences concerning trust, subjective and objective ambivalence and breadth of self-disclosure between conditions. When deciding on a privacy-utility tradeoff [32], participants might have chosen a robot that has more lenient privacy settings and is therefore more functional. Such a tradeoff has been previously observed concerning tele-operated robots [19]. In this case, participants might feel ambivalent about the robots as they have accepted that they would be distrusting towards the robot, while at the same time liking and wanting to use it. Previous research has shown that seemingly opposing attitude components are an inherent factor of robot-related attitudes—such as liking a robot but not trusting it—and it is not a contradiction to have positive and negative evaluations about a robot at the same time [56]. Another construct related to ambivalence that was tested in the current work is compensatory cognitions—operationalized by means of the Belief in a Just World scale. Compensatory cognitions may occur in order to compensate for the experienced uncertainty when experiencing ambivalence [68]. We explored whether higher ambivalence would lead to motivated compensation of uncertainty, expressed through a higher belief in a just world. However, this assumption was not supported by our data. The role of compensatory cognitions thus should be tested further [see also 56]. Possibly, ambivalence only leads to compensatory cognitions when the ambivalence under investigation is particularly relevant to the self, as is the case, e.g., with political opinions as evaluated in the original experiment connecting ambivalence and compensatory cognitions. For a robot as an attitude object, which participants did not meet and also could not expect to meet it in the future, the personal relevance might be rather low and thus not require compensatory cognitions.

Concerning correlational findings, the results obtained in Experiment 2 diverged from those obtained in Experiment 1: For instance, in Experiment 2, technology commitment correlated with many variables, e.g., likeability, trust, and

Table 2 Means, standard deviations, and correlations with confidence intervals between all measures

Variable	*M*	*SD*	1	2	3	4	5	6	7	8	9	10
1. Privacy risk	4.61	1.41										
2. Likeability	3.73	1.37	− .28***									
			[− .44, − .10]									
3. Trust	3.86	1.16	− .48***	.62***								
			[− .61, − .32]	[.49, .72]								
4. Contact intentions	3.61	1.47	− .35***	.64***	.55***							
			[− .50, − .18]	[.52, .74]	[.41, .67]							
5. Subjective ambivalence	4.17	1.60	.35***	.09	− .12	.03						
			[.17, .50]	[− .10, .27]	[− .29, .07]	[− .15, .22]						
6. Objective ambivalence	2.64	1.97	.13	.09	.00	.16*	.33***					
			[− .06, .31]	[− .10, .27]	[− .18, .19]	[− .03, .33]	[.15, .49]					
7. Breadth of self-disclosure	3.17	1.38	− .33***	.47***	.46***	.63***	− .02	.14*				
			[− .48, − .15]	[.32, .61]	[.30, .59]	[.50, .73]	[− .21, .16]	[− .04, .32]				
8. Depth of self-disclosure	3.28	1.62	− .46***	.49***	.54***	.60***	− .02	.12	.51***			
			[− .60 − .30]	[.34, .62]	[.40, .66]	[.47, .71]	[− .20, .17]	[− .07, .30]	[.36, .64]			
9. Loneliness	2.04	0.72	.16*	.08	− .05	.14	.12	.19**	.12	.00		
			[− .02, .34]	[− .11, .26]	[− .24, .13]	[− .05, .31]	[− .07, .30]	[.00, .36]	[− .07, .30]	[− .18, .19]		
10. Technology commitment	4.83	1.10	− .24***	.27***	.16*	.34***	− .17*	− .10	.14	.20**	− .05	
			[− .41, − .06]	[.09, .43]	[− .03, .33]	[.16, .49]	[− .34, .02]	[− .28, .09]	[− .05, .31]	[.01, .37]	[− .23, .13]	
11. Personal belief in a just world	4.92	1.03	− .11	.03	.21**	.07	− .12	− .18*	.01	.12	− .38***	.07
			[− .29, .08]	[− .15, .22]	[.02, .38]	[− .12, .25]	[− .30, .07]	[− .36, .00]	[− .18, .19]	[− .06, .30]	[− .53, − .21]	[− .12, .25]

M and *SD* are used to represent mean and standard deviation, respectively. Values in square brackets indicate the 99% confidence interval for each correlation. The confidence interval is a plausible range of population correlations that could have caused the sample correlation [67]. *indicates $p < .05$. ***indicates $p < .01$. ***indicates $p < .001$

subjective ambivalence, which was not the case in the context of Experiment 1. This finding indicates that technology commitment has a particular impact on attitudes towards robots when participants are involved in design decisions. That is, people high in technology commitment might be particularly interested in being part of the robot design process and might be especially prone to improvements in their robot-related attitudes when having the opportunity to make use of their expertise regarding technology. However, the sample was larger in Experiment 2 than in Experiment 1, which could be an explanation for the higher number of significant correlations. Furthermore, the significant correlation between perceived privacy risk and all dependent variables again underlines the importance of perceived privacy risk rather than actual privacy risk concerning robot-related attitudes.

6 General Discussion

In the current work, we aimed to investigate the influence of a robot's privacy settings on attitudes and behavioral intentions towards it. For this purpose, we manipulated privacy settings both in absolute terms (strict vs. lenient; Experiment 1) and in a user-centered way (i.e., providing participants with a choice vs. no choice; Experiment 2). In both experiments we investigated the influence of privacy settings on robot likeability, contact intentions, robot-related trust, attitudinal ambivalence and depth and breadth of self-disclosure.

Whereas participants did not evaluate the robot with strict privacy settings as significantly more likeable compared to the robot with lenient privacy settings in Experiment 1, choosing privacy settings seemed to have an impact on likeability in Experiment 2. Here, the robot with self-chosen privacy settings was evaluated as more likeable compared to a robot with preset privacy settings. This corresponds to the "I designed it myself" effect, which posits that things are evaluated more positively when potential users are enabled to participate in the design process [40]. The same was true for contact intentions. While privacy settings did not impact contact intentions in Experiment 1, participants seemed more eager to meet the robot when choosing the privacy settings themselves in Experiment 2, compared to the preset settings. It might be that participants rather like and want to meet a robot with which they engaged regarding some settings themselves, like in the "I designed it myself" effect, while the particular privacy settings might be secondary for likeability and contact intentions concerning a robot. However, the results concerning trust showed a different pattern.

Whereas trust towards the robot was significantly higher in the strict privacy condition compared to the lenient privacy condition in Experiment 1, there was no significant difference in terms of trust between choice conditions in Experiment 2. This might be due to the fact that the robot in the lenient privacy condition did not have the capability to engage in distrust-inducing behavior due to its restrictions. In Experiment 2, participants might have engaged in a privacy-utility tradeoff and thus did not choose the settings resulting in the utmost trustworthiness. We see descriptively a tendency to choose moderate privacy settings which speaks for the suggested privacy-utility tradeoff. We conclude that strict privacy settings contribute to higher trust towards robots, but that is not necessarily the most important factor to the users' general attitudes and behavioral intentions towards robots. Rather, users might wish to choose their own preferred tradeoff between privacy and utility which does increase general attitudes and behavioral intentions.

Furthermore, we investigated factors that might attenuate ambivalence with regards to robots which was reported in recent research [10, 27]. Despite the personal experience of conflicting thoughts and feelings (i.e., subjective ambivalence) being significantly lower concerning a robot with strict privacy settings compared to lenient privacy settings in Experiment 1, there was no difference depending on the choice condition in Experiment 2 regarding subjective ambivalence. One possible interpretation might be that with lenient privacy settings which participants might have chosen in Experiment 2, both privacy-risks and utility increase, causing an attitudinal conflict. Thus, subjective ambivalence is not reduced as participants might choose lenient privacy settings to make a tradeoff between privacy and utility. While this conflict might be reduced by choosing the privacy settings, the conflict might be re-activated during robot evaluation due to a more deliberate thinking about the positive and negative evaluations related to such choices. This would indicate two opposing effects canceling each other out. However, this is only one possible interpretation and might be further investigated in future experiments. Both in Experiment 1 and 2, experimental manipulations did not have an impact on self-reported objective ambivalence. Previous research has indicated that objective and subjective ambivalence towards robots is usually high and not significantly influenced by manipulations of robot details [10]. In the current experiments, subjective and objective ambivalence were on a medium to high level. We might conclude that choosing privacy settings does not seem to be a potential way of reducing subjective and objective attitudinal ambivalence towards robots.

Lastly, results concerning self-disclosure were partly consistent between experiments. When social robots become part of the home environment, they might be targets of self-disclosure. The collected data makes disclosers vulnerable to the transmission to third parties which could exploit them [e.g., 50]. To overcome this issue, users of social robots might prefer strict privacy settings or insist on self-chosen privacy

settings. Accordingly, we found in Experiment 1 that participants would self-disclose more intimately and for a longer time towards the social robot when the privacy settings are strict compared to lenient. Similarly, in Experiment 2, participants who chose the privacy settings themselves would self-disclose more intimate topics towards the social robot. However, there was no significant difference in the preferred duration of self-disclosure between preset and self-chosen privacy conditions in Experiment 2. This result might be explained by the strong association of self-disclosure intimacy, i.e., depth of self-disclosure, and perceived risk of the self-disclosure [18]. People are keen to protect their own intimate information more than to protect a lot of information low in intimacy as especially personal information high in intimacy in the hands of others can cause negative consequences. Therefore, more control over privacy settings might have a stronger impact on the depth of self-disclosure with which users are comfortable than on the duration of self-disclosure. We conclude that strict privacy settings and the opportunity to choose privacy settings independently might increase the willingness to self-disclose towards a robot or in the presence of a robot, especially when it comes to more personal self-disclosure. The current findings indicate that strict privacy settings as well as the opportunity to choose privacy settings both have the potential to improve robot-related attitudes and behavioral intentions such as ambivalence, likeability and the willingness for self-disclosure. However, those two manipulations seemed to influence attitudes in diverging domains. While strict privacy settings enhanced trust, attenuated subjective ambivalence, and increased the willingness to self-disclose in intimacy and duration, the choice of privacy settings seems to primarily impact robot likeability, contact intentions and the intimacy of potential self-disclosure. It seems that lenient vs. strict privacy settings primarily influence trust-related constructs. In contrast, choosing privacy settings seems to influence primarily general attitudinal aspects and general behavioral intentions, but not primarily trust-related constructs. One interpretation is that participants do not choose the strictest privacy conditions because they want to increase utility by reducing privacy. This privacy-utility tradeoff possibly activates strong positive and strong negative associations with the robot, but does not necessarily reduce privacy risk and thus has no impact on trust-related constructs. Future experiments might replicate these results in different scenarios and investigate the underlying mechanisms leading to such divergences. These results might have practical implications: To exemplify, it might be beneficial if a robot is only allowed to tighten privacy settings up automatically, but never to reduce the strictness of privacy settings as users in general prefer strict vs. lenient privacy settings. However, based on these results, we recommend to allow participants to choose privacy settings themselves and to communicate available privacy settings transparently. It even might be beneficial to compel users to deal with the privacy settings of a robot when starting the robot for the first time so that users set privacy settings they feel comfortable with which might increase the chance of long-term robot use.

6.1 Strengths, Limitations, and Future Work

The present research has numerous strengths: First, we could show that preset privacy settings (strict vs. lenient) affects especially trust-related attitudes and behavioral intentions towards robots, and that having a choice regarding privacy settings influences general attitudes and behavioral intentions towards robots. We found that participants tended to choose moderate privacy settings, which reflect a privacy-utility tradeoff on the part of the users. Due to the two-study design with the same measures, but different manipulations, the results are easily comparable and the combination of manipulations provides insights that would not have been possible independently. On a theoretical level we suggest a plausible interpretation why the manipulations of privacy settings (strict vs. lenient) in Experiment 1 and the possibility to choose (preset vs. self-chosen privacy settings) in Experiment 2 show different result patterns, which can be investigated more deeply in future work. Second, we committed to open science principles, e.g., having preregistered hypotheses and making the data and analysis code available. Moreover, the current research builds a bridge between research on assistive technologies, such as Alexa or Siri, and HRI research. While there was no actual interaction in the current scenario, the features of the introduced robot went beyond those of voice assistants by being able to move around the personal space and being a potential interaction partner with emotional expression rather than solely responding to prompts. Further, the experimental manipulation of privacy settings allowed for a standardized and systematic investigation of privacy settings which could also be used in future research. However, the chosen available privacy settings do not encompass all possible privacy settings for social robots. Thus, other privacy settings should also be tested, including those implemented in robots which are already on the market. To illustrate, it might be useful to allow for individual sensor-related privacy settings: Thereby, users could decide if they wish to have visual or auditive data stored under specific circumstances. User preferences for privacy settings might change depending on specific situations, e.g., being alone with the robot vs. having guests on a private party. Therefore, it is a strength as well as a weakness of the current work that we investigated only rather general privacy settings in our research: General privacy settings allow to explore their impact on attitudes and behavioral intentions towards a social robot from a basic research perspective. At the same time, it is important to demonstrate that indeed, user attitudes and behavioral intentions are affected by the preset

privacy settings (Experiment 1) or the opportunity to choose such settings oneself (Experiment 2).

Another critique relates to the study design: We only conducted online studies due to the COVID-19 pandemic, which also did not allow for a human–robot interaction. Thereby we could easily reach the preregistered large sample sizes, but could not control the sample characteristics. Thus, our sample consisted mostly of students. Because of the online design, the current experiments relied on text-based scenarios instead of a real-life HRI. Future research might investigate whether the results are replicable in actual HRIs and with more diverse samples. Especially end user groups, such as elderly people with increased health care needs [e.g., 70] should be taken into account in future experiments. Moreover, it is still unclear how attitudes towards the robot and data security might change during an extended time of exposure. Using an actual HRI would also allow to assess actual self-disclosure instead of self-disclosure intentions and thus increase ecological validity. To investigate self-disclosure in further detail, more comprehensive measures of self-disclosure could be used, e.g., a scale to measure the willingness to self-disclose with topics which vary in valence and intimacy [48]. Using such a scale would allow to investigate effects on specific topics and would improve our knowledge on privacy effects on more specific disclosures. Moreover, we focused only on the robot VIVA. Due to the robot scenario taken from a real-life use case we enhance the findings' internal and external validity. However, to generalize the results on other robot types, other robots than VIVA should also be examined in future.

We recommend for future studies to deepen our understanding through considering privacy settings in specific situations, including situational privacy needs. Thereby, not only recommendations for general privacy settings can be made, e.g., that medium privacy settings are in general more preferred than the most lenient privacy settings, but also situational privacy behavior of a robot can be implemented, e.g., having an automatic to set stricter privacy settings when specific circumstances are given. To illustrate, if private gatherings require more strict privacy settings than being alone with a social robot, then a robot could be trained to identify a private gathering through counting humans in the home environment and then automatically switching to stricter privacy settings if a certain threshold is reached.

To deepen our understanding of the privacy related "I designed it myself" effect, future research could also compare the opportunity to choose privacy settings compared to choosing other robot-related features. To illustrate, it would be possible that not only choosing privacy settings (e.g., strict vs. lenient) enhances likeability and contact intentions, but also choosing other robot characteristics, e.g., design features [35, 36], or general behavior (e.g., times the robot initiates contact to the user). Thereby, it could be clarified whether some of the effects occurred because of the possibility to choose any characteristic, which would speak for a general "I designed it myself" effect, or because of the privacy-related choice specifically. To sum up, we recommend future research to attempt applying the results to actual HRI and to other robot types, to other specific privacy settings (e.g., sensor data), to situational privacy settings (e.g., only one user present vs. more people present), to a broader sample, to specific user-groups (e.g., people in health-care institutions), and to broader measures of self-disclosure.

7 Conclusion

With two experiments we showed that the strictness of privacy settings and having the opportunity to choose privacy settings affects attitudes and behavioral intentions towards robots. Based on these results, we recommend to offer diverse privacy settings, individually adapted to the specific social robot under consideration. If trust-related attitudes and behavioral intentions are of essence, strict privacy settings should be provided, while in general, attitudes towards a robot may be enhanced through providing the user with the opportunity to partake in the selection of privacy settings. These privacy preferences can be individually set through an app, as suggested by other authors [5]. Future research might even consider situational privacy settings which could be automated if specific characteristics like the number of humans in the home environment are identifiable. However, automated privacy settings might make users feel uncomfortable as they might fear losing control over the privacy settings, thus, strict rules might be needed and communicated to users to enhance users' comfort using automated technology. To conclude, our work demonstrated that privacy-related concerns represent a relevant aspect of HRI which influence attitudes towards robots substantially. Both strict privacy settings as well as opportunities to control a robot's settings have the potential to improve attitudes towards robots and to increase users' willingness to interact with them.

Supplementary Information The online version contains supplementary material available at https://doi.org/10.1007/s12369-023-01043-8.

Acknowledgements The authors thank Annabelle Mielitz, Jonathan Schober, Julia Schlagheck, and Tugay Karasu for their help in manuscript preparation.

Author Contributions FE and JGS contributed to the study conception. FE, JGS, and AP contributed to the study designs. Material preparation and analysis were performed by JGS. Data collection was performed by all authors. The first draft of the manuscript was written by JGS and AP and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript. All authors agreed to be accountable for all aspects of the work in ensuring that questions related

to the accuracy or integrity of any part of the work are appropriately investigated and resolved.

Funding Open Access funding enabled and organized by Projekt DEAL. This research has been funded by the German Federal Ministry of Education and Research (BMBF) in the project 'VIVA' (Grant No. 16SV7959). The authors have no relevant financial or non-financial interests to disclose.

Data Availability All data generated or analysed during this study are included in this published article and its supplementary information files.

Declarations

Ethical Approval The current experiments were approved by the ethics committee of Bielefeld University (application No. EUB 2019-237 of 6th November 2019).

References

1. Fosch-Villaronga E, Lutz C, Tamò-Larrieux A (2020) Gathering expert opinions for social robots' ethical, legal, and societal concerns: findings from four international workshops. Int J Soc Robot 12:441–458. https://doi.org/10.1007/s12369-019-00605-z
2. Gupta SK (2015) Six recent trends in robotics and their implications. IEEE Spectrum. https://spectrum.ieee.org/six-recent-trends-in-robotics-and-their-implications. Accessed 24 June 2022
3. van den Berg B (2016) Mind the air gap. In: Gutwirth S, Leenes R, De Hert P (eds) Data protection on the move. Law, governance and technology series, vol 24. Springer, Dordrecht
4. Hassan T, Kopp S (2020) Towards an interaction-centered and dynamically constructed episodic memory for social robots. In: Companion of the 2020 ACM/IEEE international conference on human-robot interaction, pp 233–235. https://doi.org/10.1145/3371382.3378329
5. Horstmann B, Diekmann N, Buschmeier H, Hassan T (2020) Towards designing privacy-compliant social robots for use in private households: a use case based identification of privacy implications and potential technical measures for mitigation. In: Proceedings of the 29th IEEE international conference on robot and human interactive communication (RO-MAN), pp 869–876. https://doi.org/10.1109/RO-MAN47096.2020.9223556
6. Denning T, Matuszek C, Koscher K, Smith JR, Kohno T (2009) A spotlight on security and privacy risks with future household robots: attacks and lessons. In: Proceedings of the 11th international conference on Ubiquitous computing, pp 105–114. https://doi.org/10.1145/1620545.1620564
7. Dinev T, Hart P (2006) An extended privacy calculus model for e-commerce transactions. Inf Syst Res 17(1):61–80. https://doi.org/10.1287/isre.1060.0080
8. Burgoon JK (1982) Privacy and communication. Ann Int Commun Assoc 6(1):206–249. https://doi.org/10.1080/23808985.1982.11678499
9. Horstmann AC, Krämer NC (2019) Great expectations? Relation of previous experiences with social robots in real life or in the media and expectancies based on qualitative and quantitative ssessment. Front Psychol 10:939. https://doi.org/10.3389/fpsyg.2019.00939
10. Stapels JG, Eyssel F (2021) Robocalypse? Yes, please! The role of robot autonomy in the development of ambivalent attitudes towards robots. Int J Soc Robot. https://doi.org/10.1007/s12369-021-00817-2
11. Tamò-Larrieux A (2018) Designing for privacy and its legal framework, vol 40. Springer, Cham
12. Warren SD, Brandeis LD (1890) The right to privacy. Harv Law Rev 4(5):193–220
13. Van der Sloot B (2018) A new approach to the right to privacy, or how the European Court of Human Rights embraced the non-domination principle. Comput Law Secur Rev 34(3):539–549. https://doi.org/10.1016/j.clsr.2017.11.013
14. Westin AF (2003) Social and political dimensions of privacy. J Soc Issues 59(2):431–453
15. Dannemann Lundgren F (2019) New Brazilian data protection law. GRUR Int J Eur Int IP Law 8–9:752–755
16. Altman I, Taylor DA (1973) Social penetration: the development of interpersonal relationships. Holt, Rinehart & Winston, New York
17. Derlega VJ (1984) Communication, intimacy, and close relationships. Academic Press, New York
18. Omarzu J (2000) A disclosure decision model: determining how and when individuals will self-disclose. Personal Soc Psychol Rev 4(2):174–185
19. Butler DJ, Huang J, Roesner F, Cakmak M (2015) The privacy-utility tradeoff for remotely teleoperated robots. In: Proceedings of the 10th Annual ACM/ieee international conference on human–robot interaction, pp 27–34. https://doi.org/10.1145/2696454.2696484
20. Koops BJ, Leenes R (2014) Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law. Int Rev Law Comput Technol 28(2):159–171. https://doi.org/10.1080/13600869.2013.801589
21. Bygrave LA (2017) Hardwiring privacy. In: Brownsword R, Scotford E, Yeung K (eds) The Oxford handbook of law, regulation, and technology. Oxford University Press, Oxford, pp 754–775
22. Zhe D, Qinghong W, Naizheng S, Yuhan Z (2017) Study on data security policy based on cloud storage. In: 2017 IEEE 3rd international conference on big data security on cloud (bigdatasecurity), pp 145–149
23. Schafer B, Edwards L (2017) "I spy, with my little sensor": fair data handling practices for robots between privacy, copyright and security. Connect Sci 29(3):200–209. https://doi.org/10.1080/09540091.2017.1318356
24. Seiderer A, Ritschel H, André E (2020) Development of a privacy-by-design speech assistant providing nutrient information for German seniors. In: Proceedings of the 6th EAI international conference on smart objects and technologies for social good, pp 114–119
25. European Commission and European Parliament, Brussels (2021) Eurobarometer 87.1 (2017). GESIS Data Archive, Cologne. https://doi.org/10.4232/1.13738d
26. Naneva S, Sarda Gou M, Webb TL, Prescott TJ (2020) A systematic review of attitudes, anxiety, acceptance, and trust towards social robots. Int J Soc Robot 12:1179–1201. https://doi.org/10.1007/s12369-020-00659-4

27. Stapels JG, Eyssel F (2021) Let's not be indifferent about robots: neutral ratings on bipolar measures mask ambivalence in attitudes towards robots. PLoS ONE 16(1):e0244697. https://doi.org/10.1371/journal.pone.0244697
28. Lutz C, Tamó-Larrieux A (2020) The robot privacy paradox: understanding how privacy concerns shape intentions to use social robots. Hum Mach Commun 1:87–111. https://doi.org/10.30658/hmc.1.6
29. Jeong S, Alghowinem S, Aymerich-Franch L, Arias K, Lapedriza A, Picard R, Park HW, Breazeal C (2020) A robotic positive psychology coach to improve college students' wellbeing. In: 2020 29th IEEE international conference on robot and human interactive communication (RO-MAN), pp 187–194. IEEE. https://doi.org/10.1109/RO-MAN47096.2020.9223588
30. Deci EL, Ryan RM (2012) Self-determination theory. In: Van Lange PAM, Kruglanski AW, Higgins ET (eds) Handbook of theories of social psychology. Sage Publications Ltd, pp 416–436
31. Złotowski J, Yogeeswaran K, Bartneck C (2017) Can we control it? Autonomous robots threaten human identity, u31queness, safety, and resources. Int J Hum Comput Stud 100:48–54. https://doi.org/10.1016/j.ijhcs.2016.12.008
32. Burbach L, Halbach P, Plettenberg N, Nakayama J, Ziefle M, Calero Valdez A (2019) "Hey, Siri", "Ok, Google", "Alexa". Acceptance-relevant factors of virtual voice-assistants. In: 2019 IEEE international professional communication conference (ProComm), pp 101–111. https://doi.org/10.1109/ProComm.2019.00025
33. Lutz C, Schöttler M, Hoffmann CP (2019) The privacy implications of social robots: scoping review and expert interviews. Mob Media Commun 7(3):412–434. https://doi.org/10.1177/2050157919843961
34. Stange S, Hassan T, Schröder F, Konkol J, Kopp S (2022) Self-explaining social robots: an explainable behavior generation architecture for human-robot interaction. Front Artif Intell 5:866920. https://doi.org/10.3389/frai.2022.866920
35. Reich-Stiebert N, Eyssel F, Hohnemann C (2019) Exploring university students' preferences for educational robot design by means of a user-centered design approach. Int J Soc Robot 12:227–237. https://doi.org/10.1007/s12369-019-00554-7
36. Reich-Stiebert N, Eyssel F, Hohnemann C (2019) Involve the user! Changing attitudes toward robots by user participation in a robot prototyping process. Comput Hum Behav 91:290–296. https://doi.org/10.1016/j.chb.2018.09.041
37. Norton MI, Mochon D, Ariely D (2012) The IKEA effect: when labor leads to love. J Consumer Psychol 22(3):453–460. https://doi.org/10.1016/j.jcps.2011.08.002
38. Mochon D, Norton MI, Ariely D (2012) Bolstering and restoring feelings of competence via the IKEA effect. Int J Res Mark 29(4):363–369. https://doi.org/10.1016/j.ijresmar.2012.05.001
39. Kaiser U, Schreier M, Ofir C (2012) Self-customization effects on brand extensions. In: Gürhan-Canli Z, Otnes C, Zhu RJ (eds) NA-advances in consumer research, vol 40. Association for Consumer Research, Duluth, pp 53–57
40. Franke N, Schreier M, Kaiser U (2010) The "I designed it myself" effect in mass customization. Manag Sci 56(1):125–140. https://doi.org/10.1287/mnsc.1090.1077
41. Kaplan KJ (1972) On the ambivalence-indifference problem in attitude theory and measurement: a suggested modification of the semantic differential technique. Psychol Bull 77(5):361–372. https://doi.org/10.1037/h0032590
42. Derlega VJ, Metts S, Petronio S, Margulis ST (1993) Self-disclosure. Sage Publications Inc.
43. Collins NL, Miller LC (1994) Self-disclosure and liking: a meta-analytic review. Psychol Bull 116(3):457–475. https://doi.org/10.1037/0033-2909.116.3.457
44. Joinson AN, Reips UD, Buchanan T, Schofield CBP (2010) Privacy, trust, and self-disclosure online. Hum Comput Interact 25(1):1–24. https://doi.org/10.1080/07370020903586662
45. Uchida T, Takahashi H, Ban M, Shimaya J, Yoshikawa Y, Ishiguro H (2017) A robot counseling system—what kinds of topics do we prefer to disclose to robots? In: 2017 26th IEEE international symposium on robot and human interactive communication (RO-MAN), pp 207–212
46. Ho A, Hancock J, Miner AS (2018) Psychological, relational, and emotional effects of self-disclosure after conversations with a chatbot. J Commun 68(4):712–733. https://doi.org/10.1093/joc/jqy026
47. Duan YE, Yoon MJ, Liang ZE, Hoorn JF (2021) Self-disclosure to a robot: only for those who suffer the most. Robotics 10(3):98. https://doi.org/10.3390/robotics10030098
48. Penner A, Eyssel F (2022) Germ-free robotic friends: loneliness during the COVID-19 pandemic enhanced the willingness to self-disclose towards robots. Robotics 11(6):121. https://doi.org/10.3390/robotics11060121
49. Rossi A, Giura V, Di Leva C, Rossi S (2021) I know what you would like to drink: benefits and detriments of sharing personal info with a bartender robot. arXiv preprint https://arxiv.org/abs/2103.13337
50. Syrdal DS, Walters ML, Otero N, Koay KL, Dautenhahn K (2007) He knows when you are sleeping-Privacy and the personal robot companion. In: Proc. workshop human implications of human-robot interaction, association for the advancement of artificial intelligence (aaai'07), pp 28–33
51. Reeves B, Nass C (1996) The media equation: how people treat computers, television, and new media like real people. Cambridge University Press, UK
52. Bazarova NN, Choi YH (2014) Self-disclosure in social media: extending the functional approach to disclosure motivations and characteristics on social network sites. J Commun 64(4):635–657. https://doi.org/10.1111/jcom.12106
53. Geambasu R, Kohno T, Levy AA, Levy HM (2009) Vanish: increasing data privacy with self-destructing data. In: USENIX security symposium, vol 316, pp 10–5555.
54. Petrak B, Stapels JG, Weitz K, Eyssel F, André E (2021) To move or not to move? Social acceptability of robot proxemics behavior depending on user emotion. In: 2021 30th IEEE international conference on robot & human interactive communication (RO-MAN), pp 975–982. IEEE
55. Stange S, Kopp S (2021) Effects of referring to robot vs. user needs in self-explanations of undesirable robot behavior. In: Companion of the 2021 ACM/IEEE international conference on human-robot interaction, pp 271–275. https://doi.org/10.1145/3434074.3447174
56. Stapels J (2022) Ambivalence in attitudes towards robots. Dissertation, University of Bielefeld. https://doi.org/10.4119/unibi/2960732
57. Reysen S (2005) Construction of a new scale: the Reysen likability scale. Soc Behav Personal Int J 33(2):201–208. https://doi.org/10.2224/sbp.2005.33.2.201
58. Salem M, Eyssel F, Rohlfing K, Kopp S, Joublin F (2013) To err is human (-like): effects of robot gesture on perceived anthropomorphism and likability. Int J Soc Robot 5(3):313–323. https://doi.org/10.1007/s12369-013-0196-9
59. Touré-Tillery M, McGill AL (2015) Who or what to believe: trust and the differential persuasiveness of human and anthropomorphized messengers. J Mark 79(4):94–110. https://doi.org/10.1509/jm.12.0166
60. Eyssel F, Kuchenbrandt D (2012) Social categorization of social robots: anthropomorphism as a function of robot group membership. Br J Soc Psychol 51(4):724–731. https://doi.org/10.1111/j.2044-8309.2011.02082.x
61. Priester JR, Petty RE (1996) The gradual threshold model of ambivalence: relating the positive and negative bases of attitudes to subjective ambivalence. J Personal Soc Psychol 71(3):431. https://doi.org/10.1037/0022-3514.71.3.431

62. Thompson MM, Zanna MP, Griffin DW (1995) Let's not be indifferent about (attitudinal) ambivalence. In: Petty RE, Krosnick JA (eds) Attitude strength: antecedents and consequences, Ohio State University Attitudes and Persuasion, vol 4. Psychology Press, New York and London, pp 361–386
63. Malhotra NK, Kim SS, Agarwal J (2004) Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. Inf Syst Res 15(4):336–355. https://doi.org/10.1287/isre.1040.0032
64. Neyer FJ, Felber J, Gebhardt C (2012) Entwicklung und Validierung einer Kurzskala zur Erfassung von Technikbereitschaft. Diagnostica 58(2):87–99. https://doi.org/10.1026/0012-1924/a000067
65. Lamm H, Stephan E (1986) Zur Messung von Einsamkeit: Entwicklung einer deutschen Fassung des Fragebogens von RUSSELL und PEPLAU. Psychol Prax 3:132–134
66. Cohen J (1988) Statistical power analysis for the behavioral analyses. Laurence Erlbaum Associates, Hillsdale
67. Cumming G (2014) The new statistics: why and how. Psychol Sci 25(1):7–29. https://doi.org/10.1177/0956797613504966
68. DeMarree KG, Wheeler SC, Briñol P, Petty RE (2014) Wanting other attitudes: actual-desired attitude discrepancies predict feelings of ambivalence and ambivalence consequences. J Exp Soc Psychol 53:5–18. https://doi.org/10.1016/j.jesp.2014.02.001
69. Dalbert C (2000) Beliefs in a just world questionnaire. In: Maltby J, Lewis CA, Hill A (eds) Commissioned reviews of 250 psychological tests. Edwin Mellen Press, Lampeter, pp 461–465
70. Koceski S, Koceska N (2016) Evaluation of an assistive telepresence robot for elderly healthcare. J Med Syst 40(5):1–7. https://doi.org/10.1007/s10916-016-0481-x

Julia G. Stapels was a researcher and PhD student at the research group "Applied Social Psychology and Gender Research" at the Center for Cognitive Interaction Technology (CITEC) during the research work presented here. She worked in the project VIVA (2018 - 2021) where a novel, trustworthy and friendly social robot was developed, funded by the German Federal Ministry of Education and Research. Dr. Stapels received her Master's degree in Psychology from University of Cologne in 2017 and her PhD in Psychology in 2021 from Bielefeld University, Germany. She is currently a data steward at TU Dortmund University, Germany.

Angelika Penner is currently a PhD student in the research group "Applied Social Psychology and Gender Research" at the Center for Cognitive Interaction Technology (CITEC) at Bielefeld University, Germany. Angelika Penner received an M.Sc. degree in psychology from Bielefeld University. Her research interests are social robotics and human-robot interaction. In her PhD project she investigates self-disclosure in human-robot interaction with experimental methods and a theoretical foundation rooted in social psychology.

Niels Diekmann is an Attorney of Law specializing in information technology law (esp. cloud computing and artificial intelligence) as well as data protection. He was a researcher at the University of Applied Science Bielefeld in the period from 2018 to 2020. He worked in the project VIVA and GUIDE. Within the Guide project a guideline was developed and published to provide scientists with guidance on complying and managing data protection in projects involving human-technology interaction. The project was conducted in cooperation with the Fraunhofer Institute IOSB Karlsruhe and funded by the German Federal Ministry of Education and Research. Niels Diekmann has studied at Bielefeld University and was admitted to the bar for the first time in 2017. He is currently a Legal Counsel in an international tech company.

Friederike Eyssel is professor of psychology and head of the research group "Applied Social Psychology and Gender Research" at the Center for Cognitive Interaction Technology (CITEC), Bielefeld University, Germany. Friederike Eyssel earned her Masters degree in Psychology from University of Heidelberg in 2004. She received her PhD in Psychology from Bielefeld University in 2007. Dr. Eyssel has held visiting professorships in social psychology at the University of Münster, the Technical University of Dortmund, the University of Cologne, and New York University Abu Dhabi. Dr. Eyssel is passionate about basic and applied social psychological research and she is interested in various research topics ranging from social robotics, trust, and acceptance of novel techlologies to attitudes and attitude change. Crossing disciplines, Dr. Eyssel has published her research in leading venues the field of social psychology and human-robot interaction. She is co-author of various textbooks on social robots, among them "HRI: An introduction (2020, Cambridge University Press), "Robots in Education" (2021, Routledge), and "Theory and practice of sociosensitive and socioactive systems" (2022, Springer).