STARS

Human-Machine Communication

Volume 1 *Inaugural Volume* Article 6

2020

The Robot Privacy Paradox: Understanding How Privacy Concerns Shape Intentions to Use Social Robots

Christoph Lutz
BI Norwegian Business School

Aurelia Tamò-Larrieux
University of Zurich

HUMAN-MACHINE COMMUNICATION

Human-Machine Communication
Volume 1, 2020
https://doi.org/10.30658/hmc.1.6

The Robot Privacy Paradox: Understanding How Privacy Concerns Shape Intentions to Use Social Robots

Christoph Lutz[1] **and Aurelia Tamó-Larrieux**[2]

1 Department of Communication and Culture, BI Norwegian Business School, Nordic Centre for Internet and Society, Oslo, Norway
2 Center for Information Technology, Society, and Law, University of Zurich, Zurich, Switzerland

Abstract

Conceptual research on robots and privacy has increased but we lack empirical evidence about the prevalence, antecedents, and outcomes of different privacy concerns about social robots. To fill this gap, we present a survey, testing a variety of antecedents from trust, technology adoption, and robotics scholarship. Respondents are most concerned about data protection on the manufacturer side, followed by social privacy concerns and physical concerns. Using structural equation modeling, we find a privacy paradox, where the perceived benefits of social robots override privacy concerns.

Keywords: social robots, privacy, trust, survey

Introduction

Does the privacy paradox translate to the use of social robots? In other words, is there a robot privacy paradox? In this article, we empirically investigate the link between privacy concerns and the intention to use social robots. As social robots are increasingly interacting with us in our daily environment (Fong et al., 2003; Gupta, 2015; Van den Berg, 2016), the advantages and concerns of close human-machine interaction have become a topic of public debate. A key concern triggered by human interaction with social robots is related to users' privacy (Lutz & Tamò, 2018). As social robots function based on data analysis and have greater mobility and autonomy than static devices, it is no surprise that literature has started to investigate their privacy implications on a descriptive level (Calo, 2012; Kaminski, 2015; Kaminski et al., 2017; Lutz & Tamò, 2015; Rueben, Grimm, et al., 2017; Sedenberg et al., 2016). Yet, empirical evidence on privacy concerns and privacy implications of social robots among non-experts (i.e., individuals largely unfamiliar with robots) is scarce. While

ISSN 2638-6-2X (print)/ISSN 2638-6038 (online)

www.hmcjournal.com

a few surveys have looked at trust in social robots (Alaiad & Zhou, 2014) and general attitudes toward them (Eurobarometer, 2012; Liang & Lee, 2017), privacy has mostly been discussed in conceptual terms (Calo, 2012, 2016; Lutz & Tamò, 2018; Rueben, Grimm, et al., 2017).

In this article, we present the results of a survey that aimed at understanding the general public's privacy concerns about social robots and how these concerns affect use intention. The findings point to the need to differentiate privacy types and to the important role of the social environment in shaping users' attitudes about this new technology.

In the course of the article, we first define the term "privacy" and provide an overview of previous literature on the topic of privacy in the context of social robots. We will ground the definition in previous research about online privacy and privacy in general to reach a more holistic understanding of the phenomenon. Subsequently, we will present the research model to be tested in the survey and develop the hypotheses. We then describe the survey methodology, including the sample, data analysis approach, and measurement, and present the survey results. Finally, we discuss the limitations of our approach and contextualize the findings.

Literature Review

Defining Privacy Concerns in the Context of Social Robots

Despite new technological developments and a recent surge of interest, privacy scholarship can draw on a long academic tradition (Altman, 1975; Warren & Brandeis, 1890; Westin, 1967). Today, privacy is a multidisciplinary research field. Disciplines involved in its study include communication, computer science, psychology, sociology, information systems, economy, and law (Pavlou, 2011). However, this multitude of perspectives complicates a common understanding of the central construct. As Solove (2008, p. 1) points out:

> privacy is a sweeping concept, encompassing (among other things) freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations. Philosophers, legal theorists, and jurists have frequently lamented the great difficulty in reaching a satisfying conception of privacy.

In this article, we rely on Bygrave's (2002) distinction of privacy aspects or types and apply them in the context of social robots. The first type we consider is *physical privacy* and the notion of non-interference (dating back to the early understanding of privacy according to Warren & Brandeis, 1890). Physical privacy considerations revolve around "physical access to an individual and/or the individual's surroundings and private space" (Smith et al., 2011, p. 990). According to Calo (2012), who offers a useful privacy typology for social robots, issues related to physical privacy are linked to a robot's ability to enter physical personal spaces, such as bedrooms and bathrooms. Since robots are increasingly employed in homes, for example as household assistants, they might be exposed to sensitive

or compromising situations. Similarly, robots might have access to vulnerable population groups and their habits, such as children, the elderly, and the infirm. In this sense, physical privacy in the context of social robots relates to the notion of "freedom from" (Koops et al., 2016), which incorporates the idea that an individual remains unobserved in private spaces.

Physical privacy can be distinguished from informational privacy (Smith et al., 2011). The latter follows Westin's (1967) famous definition of privacy as a means to achieve self-realization and thus being able to control information about ourselves. Informational privacy can further be divided into two subcategories: one that relates to institutional threats and one that relates to social threats (Raynes-Goldie, 2010; Young & Quan-Haase, 2013). While *institutional informational privacy* includes privacy considerations about the processing of data by institutions (e.g., robot manufacturers, government agencies, and third parties such as data brokers or cloud providers), social informational privacy revolves around the processing of data by private individuals (e.g., familiar users, hackers). Surveillance is a dominant concern with regard to informational privacy, both institutional and social (Calo, 2012). As modern robots are equipped with innovative sensors and processors, enabling more advanced observation capabilities than humans, they potentially could be used for spying and sophisticated "background" data collection (i.e., without awareness or consent by users and bystanders).

Privacy can also be understood as "a selective control of access to the self or to one's group" (Altman, 1975, p. 18). We call this group *social informational privacy*. While in this article we understand access to the self broadly, we are interested in social "freedom from" forms of privacy (Koops et al., 2016) in the sense of informational boundary management. These forms link back to the physical privacy concerns of having one's own space free from intrusion (Kaminski, 2015; Kaminski et al., 2017). However, the notion of boundary management is broader than "freedom from" surveillance, as it understands privacy as a protection of individuals' agency to make their own life choices and thus ultimately as "freedom from unreasonable constraints on the construction of identity" (Carnevale, 2016, p. 147). Social informational privacy concerns rest on the ability of a user to understand how information shared with the social robot is processed, especially considering the anthropomorphic effect of social robots. This effect has been widely recognized in the literature on social robots (Darling, 2016; Weiss et al., 2009), also as an important aspect regarding privacy (Calo, 2012; Syrdal et al., 2007). Studies in the field of human-robot-interaction have shown that humans tend to anthropomorphize or zoomorphize social robots (Fong et al., 2003). This increases their pervasiveness compared with other connected technology (Turkle, 2011), in the sense that humans might feel more inclined to see the robots as companions or friends. In turn, they will be more likely to entrust the robots with personal, potentially sensitive information. Social informational privacy thus includes aspects of boundary management between a social robot and a user (e.g., can secret information such as passwords be revealed to the robot), touching on aspects of interdependency and bonding (Calo, 2012). However, social informational privacy concerns not only relate to the interaction between the user and the robot itself but also to the interaction between individuals through a robot, for example when a robot is hacked or surveillance takes place through a telepresence robot.

Empirical Research on Privacy Concerns in the Context of Social Robots

As mentioned above, empirical research on privacy concerns in the context of social robots exists but remains in its infancy. For example, an exploratory study based on qualitative interviews investigated privacy perceptions of the social workplace robot Snackbot (Lee et al., 2011). The interviews revealed that most participants were not able to grasp the types of data Snackbot collects and failed to differentiate between sensed data ("what the robot sees/hears") and inferred information ("what the robot knows," p. 182). The authors also found that Snackbot's anthropomorphic form could mislead participants in their understanding of the capabilities to record information. Specifically, participants did not expect that Snackbot could sense objects or people behind it.

Other surveys explored the issue of information disclosure in human-robot interactions. In a study conducted by Syrdal et al. (2007), participants' fear of robots storing and accessing sensitive information about individuals' behavior was considered a "necessary evil" that had to be tolerated so long as the social robots brought them benefits. Similarly, Butler et al. (2015) analyzed the privacy-utility tradeoff for teleoperated robots, with the aim of reducing "the quantity or fidelity of visual information received by the teleoperator to preserve the end-user's privacy" (p. 27), while still providing sufficient information for the robot to be able to fulfill its tasks. The authors provide a framework for understanding what visual filters may be applied to balance the privacy needs of the participants with the information needed to perform actions by the teleoperator. Studies on telepresence robotics have also been conducted with non-academic participants. Krupp et al. (2017) carried out in-depth focus groups (13 participants, 3 sessions, 2 hours long) discussing privacy in telepresence robotics. Privacy concerns expressed by the participants ranged between fear of hackers infiltrating the systems, fear of constant monitoring and recording of embarrassing moments, and fears of becoming prey to even more personalized marketing practices.

In addition, some general population surveys have assessed citizens' attitudes toward robots, including potential concerns (e.g., Eurobarometer, 2012, 2015; Madden & Rainie, 2015). While a majority of respondents in the European Union had a positive opinion of robots (64%), a common fear was robots stealing people's jobs (70%). Moreover, a majority of respondents felt uncomfortable with the thought of robots providing companionship to older people and with robots being used for surgeries on them personally (Eurobarometer, 2015). The latter findings might be connected to perceptions of privacy, although the survey did not explicitly ask for privacy concerns. In the US, Liang and Lee (2017) investigated individuals' fear of robots and artificial intelligence based on national representative data. They found that about one fourth of the population had heightened fear levels and that fear of robots and artificial intelligence was positively correlated with other types of fear, including fear of government drone use.

Across this literature, few quantitative and survey-based studies have assessed privacy concerns, their antecedents and outcomes (Lutz et al., 2019). Thus, we lack knowledge about whether established privacy theories could prove useful for social robots. We also know little about non-expert opinions and concerns about social robots. This lack of knowledge could be problematic, as social robots are sometimes introduced without a thorough assessment of potential user concerns. Our contribution tries to overcome some of these gaps.

Trust and Its Link to Privacy

Trust is a complex phenomenon and so is its link to privacy (Waldman, 2018). On the one hand, and from a social informational privacy perspective, privacy allows psychological release functions and enables interpersonal relationships that are built upon trust and trusting beliefs (Tamò-Larrieux, 2018; Westin, 1967). On the other hand, and from an institutional privacy perspective, privacy features of services and products enhance consumer trust in the provider, which in turn is a key element for economic success (Hartzog, 2018; Tamò-Larrieux, 2018). In our survey, we rely on the conventional definition of trust as "a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviors of another" (Rousseau et al., 1998, p. 395). This definition aligns with Möllering's (2001) conceptualization of trust as a three-step mental process of expectation, interpretation, and suspension. The release of private information to a social robot requires trust, as such a release requires a favorable expectation of an outcome that is uncertain. The interpretation of whether the outcome will be favorable or not can rely on various rational and emotional elements (or a mix thereof); in the end, a user must have enough "good reasons" to trust to interact with a social robot. Möllering (2001) calls the moment in which the interpretation becomes accepted and the unknowable momentarily certain "suspension." Suspension represents an element of faith toward the outcome and "enables the leap of trust" (Möllering, 2001, p. 414).

Given its importance, policymakers are trying to establish trust in new technologies by enacting ethical guidelines. In particular, the rise of artificial intelligence (AI) has pushed the European Commission and the global community to establish ethical guidelines that promote trustworthy AI (Delcker, 2019; European Commission, 2018). Social robots are and will be equipped with AI-systems, which is why the adherence to ethical principles (e.g., respect for human autonomy, fairness, explicability, prevention of harm) of AI likewise affects the development of social robots. We consider privacy and data protection important aspects of ethical and trustworthy technology but cannot fully do justice to this emerging literature in ethics and AI here.

Model and Theoretical Development

Based on our discussion of the privacy literature above, as well as adjacent work on technology acceptance and trust in the context of robots (Alaiad & Zhou, 2014), we propose the following research model (Figure 1).

In our model, behavioral intention is the key dependent construct. We did not include actual behavior because few of our respondents could be expected to have experience in interacting with robots, thus making behavioral assessments unreliable and speculative. Attitudes are represented by privacy concerns, trusting beliefs, perceived benefits of robots, and scientific interest. Social psychological theories, such as the theory of planned behavior (TPB), have stressed the importance of social influence in explaining behavioral intentions. Social influence, or subjective norm (the two are often used synonymously), describes the "perceived social pressure to perform or not to perform the behavior" (Ajzen, 1991, p. 188). As social robots are employed in social settings, we included social influence as an

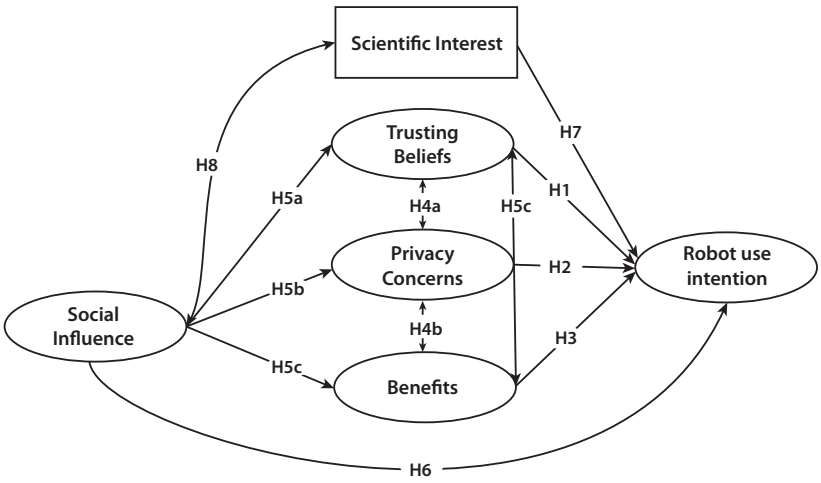

FIGURE 1 Research Model

independent construct in the model affecting use intention, trusting beliefs, privacy concerns, and perceived benefits. Finally, we included scientific interest as an attitudinal control variable affecting the intention to use social robots and being itself influenced by social influence. In the following paragraphs, we explain the model and present the hypotheses.

Among the attitudinal constructs, trust, and more specifically trusting beliefs, should be associated with robot use intentions. Trusting beliefs contain several subdimensions, the most important of which are a trustor's competence, benevolence, and integrity beliefs (McKnight et al., 2002). In other words, to form trust, the trustor must think that the trustee is competent, benevolent, and honest. If this is the case, individuals are more likely to develop trusting intentions, which will eventually result in a certain trusting behavior such as technology adoption. Based on this mechanism established in the trust literature, we propose the following hypothesis. We focus on trusting beliefs and the distinction of competency, benevolence, and integrity because such a conceptualization is easier to operationalize than, for example, Möllering's (2001) leap of trust approach.

H1: *Trusting beliefs in robot manufacturers have a positive effect on robot use intentions.*

Overcoming privacy concerns seems to be an initial requirement for the intention to start using social robots. When citizens perceive the privacy risks of social robots to be high or when they have had adverse experiences with social robots, we expect their intention to adopt them to decrease. At the same time, extensive research on online privacy and self-disclosure has found that individuals' privacy attitudes—including concerns—are often not in line with their behavior (Kokolakis, 2017). Despite substantial privacy concerns, many users of social media and other online services disclose a lot of sensitive information and engage superficially in privacy protection behavior. This misalignment between online privacy attitudes and behavior has been termed the "privacy paradox" (Barnes, 2006). A range of empirical studies has found a privacy paradox but some studies, especially newer ones, reported significant effects between privacy attitudes and behavior, thus rejecting the notion of the privacy paradox. Kokolakis offers a systematic assessment of this literature and shows

the inconclusive empirical evidence. Given the novelty of the topic (social robots), current low adoption rates, and our focus on intention rather than behavior as the dependent variable, we would expect privacy considerations to have a significant effect on use intention.

H2: *Privacy concerns about robots have a negative effect on robot use intentions.*

As shown in the literature review, we identify three key aspects of privacy—physical privacy, institutional informational privacy, and social informational privacy—that we apply to the context of social robots (summarized in Table 1). We check how each type affects use intention differently. We would expect that more familiar concerns might deter people more from robots than unfamiliar or even intangible concerns. In that sense, many citizens will be familiar with informational privacy concerns (both institutional and social) through their Internet and social media use, but will have limited familiarity with robots' physical risk potential. Thus, we expect differentiated roles of the three privacy concerns considered.

TABLE 1 Overview of Privacy Aspects Considered

Privacy aspects	Description
Physical privacy	Privacy considerations that revolve around non-interference by social robots themselves and their interaction with physical objects and spaces (e.g., by entering private rooms and using personal objects).
Institutional informational privacy	Privacy considerations that revolve around information control and data protection from and data collection practices by institutions, in particular social robot manufacturers, government agencies, and third parties (data brokers, cloud storage providers).
Social informational privacy	Privacy considerations that revolve around access to a person and data protection from and data collection practices by individuals (e.g., other users, hackers).

Within the privacy paradox literature, the privacy calculus is the dominant theoretical explanation (Dinev & Hart, 2006). According to this approach, users perform a mental calculus weighing the risks and benefits of an online technology against each other. If the benefits outweigh the risks, they will start or keep using the technology. In a similar vein, if social robots are perceived as extremely useful for someone's personal life, individuals will be more likely to develop use intentions, despite potential privacy concerns. In our case, we considered two key benefits of social robots: functional benefits (Lin, 2012) and emotional benefits (Yu et al., 2015). For the analysis we consider them in conjunction. Based on previous research (Alaiad & Zhou, 2014) and one of the core premises of TPB, we expect perceived benefits to have pronounced and comparatively strong effects on use intentions.

H3: *Perceived benefits of social robots have a positive effect on social robot use intentions.*

In our model, privacy concerns, trusting beliefs, and perceived benefits are all conceptualized as attitudes. We understand the relationship between these constructs as correlational associations rather than causal effects. Previous research in different online contexts has

specified the relationship between privacy and trust in both directions. Privacy concerns can lower trust in a service provider (Bart et al., 2005; Beldad et al., 2010; Hoffmann et al., 2014) but lowered levels of trust might also result in heightened privacy concerns (Krasnova et al., 2010). In our case, we would argue that privacy concerns can lower trust in a social robot manufacturer. If users or potential users worry that a social robot manufacturer cannot protect their data and privacy to a sufficient extent, they will potentially challenge the manufacturer's competence, benevolence, and integrity, thus having lowered trust. At the same time, trusting beliefs might decrease privacy concerns or the two might mutually enforce each other. Similarly, an increase in privacy concerns might result in the perceived benefits being less salient and a mental reconfiguration of the perceived benefits might affect someone's privacy concerns. Finally, we think that the perceived benefits and trust go hand in hand as well, leading us to hypotheses H4a–H4c.

H4a: *Privacy concerns about social robots correlate negatively with trusting beliefs in social robot manufacturers.*

H4b: *Privacy concerns about social robots correlate negatively with perceived benefits of social robots.*

H4c: *Trusting beliefs about social robots correlate positively with perceived benefits of social robots.*

As mentioned, social influence, or subjective norm, describes the "perceived social pressure to perform or not to perform the behavior" (Ajzen, 1991, p. 188). Thus, it refers to the social environment and its expectations toward an individual. Since trusting beliefs, privacy concerns, and perceived benefits of social robots do not form in a social vacuum, we hypothesize that they are all affected by social influence. More specifically, we expect an encouraging and technology-affine social environment to enhance trust, reduce privacy concerns, and make the perceived benefits of social robots more salient.

H5a: *Social influence has a positive effect on trusting beliefs about social robots.*

H5b: *Social influence has a negative effect on privacy concerns about social robots.*

H5c: *Social influence has a positive effect on perceived benefits of social robots.*

Social influence or subjective norm has proven to be an important predictor of behavioral intention in TPB (McEachan et al., 2011). Similarly, theories of technology adoption have stressed the importance of social factors, for example within the technology acceptance model framework (Venkatesh & Morris, 2000; Venkatesh, Morris, Davis, et al., 2003). In this understanding, social influence should enhance individuals' behavioral intention to adopt a new technology. Social robots, as a technology that is not yet widely adopted, will likely be adopted earlier when someone's network expects and encourages their use. Thus, citizens who are part of more social robot-friendly communities will have higher intentions to use them.

H6: *Social influence has a positive effect on social robot use intentions.*

We included scientific interest as a control variable. More scientifically interested citizens will be more up-to-date with current technological developments, also regarding social robots. As social robots are still not a mainstream technology, we assessed scientific interest as a proxy for awareness and knowledge of social robot technology. The rationale for a positive effect is that scientifically interested citizens will be better able to assess the benefits and risks of the technology, including the privacy risks. They might also be more technologically curious and open-minded, having higher willingness to try out social robots despite a lack of widespread adoption. In that sense and based on diffusion of innovation theory (Rogers, 2003), scientifically interested citizens should be more likely to be early adopters of social robots. By including scientific interest, we follow other survey-based studies (Eurobarometer, 2012).

H7: *Scientific interest has a positive effect on social robot use intentions.*

Finally, as scientific interest depends on the social milieu and environment, we hypothesize that these variables will positively correlate with each other. Again, we specify this relationship as a correlational association rather than a causal one. A social environment that is positive toward social robots and encourages their use might stimulate someone's general scientific interest. Similarly, according to homophily theory (McPherson et al., 2001), scientifically interested individuals might prefer a social environment that is positive toward social robots.

H8: *Scientific interest and social influence correlate positively.*

Methods

To test the model in Figure 1, we used a survey-based approach. We think that surveys are a useful tool to assess individuals' perceptions and beliefs, allowing for descriptive and correlational analyses. Moreover, in a systematic literature on privacy in the context of robots, the authors found that very few studies rely on surveys, so that limited evidence about privacy attitudes and concerns is available from a quantitative perspective (Lutz, Schöttler, et al., 2019).

Sample

We rely on data collected through a survey on Amazon Mechanical Turk (MTurk) in June 2016. Participants were all residents in the United States (US).[1] They were offered a monetary incentive of 2 US Dollars and survey completion took 15 minutes on average. Thus,

1 We are conscious that our position as European researchers might result in cultural bias in the interpretation of data collected in the US. However, such bias is probably mitigated by our extensive collaboration with US-based researchers, by our experience with analyzing US-based data across several projects, and by having spent considerable time at US institutions through research stays, conferences, and workshops. Despite not removing cultural bias entirely, we hope that our familiarity with the US context and culture has reduced inherent bias.

the average hourly wage for filling out the survey was approximately 8 US Dollars. 501 respondents started the survey, 480 of whom are included in the structural equation model and had no or very few missing values. 54.5% of the respondents were male, 45% female, and 0.5% (two respondents) identified as other. The respondents were relatively highly educated, with 35% having some college education, 38% a bachelor's degree, 8% a master's degree, and 2% a doctorate. Only 16% had a high school degree as their highest degree and 1% responded with "other." The average age was 34 (median 32), with a range between 18 and 74 years and a standard deviation of 10.5 years. Thus, the sample is not representative of the US general population or US adult population. The questionnaire was aimed at non-experts to capture the general privacy concerns associated with social robots.

Measurement

To make the questions relatable and prime the respondents to answer the questions for social robots (rather than industrial and other non-social robots), we showed pictures of different social robots interacting with people at the very beginning of the survey (Appendix A). The wording of all items is shown in Appendix B.

We used four items to measure respondents' intention to use social robots. A sample item was: *"I would very much like to have such a robot at home."* The scales used to measure trusting beliefs (McKnight et al., 2002) and social influence (Venkatesh, Morris, Davis, et al., 2003) were derived from well-established models. They were adapted to the context of social robots. The measures for perceived benefits were taken from the Special Eurobarometer 382 and 427 surveys on public attitudes toward robots (Eurobarometer, 2012, 2015). Scientific interest was measured with one item from Eurobarometer (2012). The measures for informational and global privacy concerns were based on previous studies (Malhotra et al., 2004; Stutzman et al., 2011), but adapted to the context of social robots. Within the global privacy concerns scale, the first item (*"Overall, I see a real threat to my privacy due to the robot."*) assesses privacy in particular, while the remaining three items capture concerns more broadly. Nevertheless, all items load neatly on one factor, with good reliability and convergent validity values (Cronbach's α of 0.90, and average variance extracted—AVE—of 0.71). Thus, we opted to retain this scale instead of relying on a less robust single-item measurement. Within the seven informational privacy concerns items, three items refer to social informational privacy concerns and four items to institutional informational privacy concerns. The scale for physical concerns was self-developed because we did not encounter studies which contained such a scale. However, the question prompt was adapted from Stutzman et al. (2011). Physical privacy concerns were measured with five items.

We relied on 5-point Likert scales ranging from "strongly disagree" to "strongly agree" for all items, except for privacy concerns. Here, respondents could assess their concern on a 5-point scale ranging from "no concern at all" (1) to "very high concern" (5). All scales reveal good measurement properties in terms of internal consistency, reliability, and validity. The measurement model (Appendix C, Table B) thus satisfies the necessary conditions to report the structural model, displaying both convergent and discriminant validity (Bollen, 1989; Fornell & Larcker, 1981; Netemeyer et al., 2003). As the only exception for discriminant validity, the squared correlation between perceived benefits and intentions exceeds the AVE of benefits by 0.01 (Appendix C, Table C). We decided to keep these two

constructs as separate because of their theoretical importance, distinct conceptualization, and because of the correlation being only very little above the threshold.

Methodological Approach

We relied on structural equation modeling (SEM) to test the research model, combining advantages of confirmatory factor analysis and regression analysis. We used robust maximum-likelihood estimation (MLR) in MPlus (Version 7) to account for non-normality, heteroscedasticity, and other possible sources of distortion (Byrne, 2012). All models reported had sufficient goodness of fit indices, with the overall privacy concerns model being the least good: Chi-Square = 508.4; degrees of freedom = 213; Root mean square error of approximation (RMSEA) = 0.054; Comparative fit index (CFI) = 0.95; Tucker-Lewis index (TLI) = 0.94; Standardized root mean square residuals (SRMR) = 0.045.

Results

Before turning to the structural model, we present descriptive results. As outlined before, we distinguish three types of privacy concerns: *physical privacy concerns*, *institutional informational privacy concerns*, and *social informational privacy concerns*. In addition, we included a measure for overall privacy concerns. In the following comparisons, it is important to remember that the wording of the different privacy constructs varies from more moderate to more extreme, depending on the risk described. Thus, the comparisons have to be interpreted carefully. The arithmetic means for *physical privacy concerns* range from 1.90 (the social robot asking personal questions), to 2.56 (the social robot damaging or dirtying personal belongings), with a global average of 2.22. This indicates low concern. The arithmetic means for *institutional informational privacy concerns* range from 3.70 (insufficient data protection), to 3.74 (selling data), with a global average of 3.72. This indicates high concern. The arithmetic means for *social informational privacy concerns* range from 2.93 (stalking), to 3.53 (hacking), with a global average of 3.17. This indicates moderate concern. Finally, the global privacy concerns measure lies in between informational privacy concerns on the one hand and physical privacy concerns on the other hand, with a global average of 2.61.

The findings indicate that the respondents are most concerned about institutional aspects of privacy (i.e., data protection on the side of the manufacturers). They seem to be unconcerned about physical privacy. However, they are somewhat concerned about other users using the social robot for malicious purposes such as stalking or hacking. Overall, respondents have moderate privacy concerns about social robots.

The model for physical privacy concerns is shown in Figure 2. Trusting beliefs and privacy concerns have no significant effect on robot use intention, rejecting H1 and H2. However, perceived benefits have a positive influence on social robot use intention, supporting H3. Physical privacy concerns, trusting beliefs and perceived benefits correlate significantly and in the expected direction with each other, thus supporting H4. Physical privacy concerns are not affected by social influence, but social influence has the predicted effect on trusting beliefs and perceived benefits, partially supporting H5. Social influence has a positive and significant effect on robot use intention, supporting H6. Finally, scientific interest

has no significant effect on robot use intention, rejecting H7, but is itself positively affected by social influence, supporting H8.

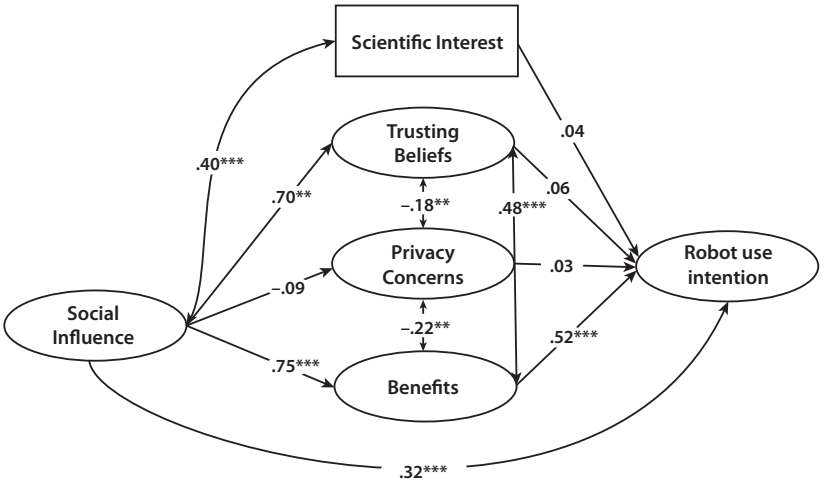

FIGURE 2 Physical Privacy Concerns Model

The models for institutional and social informational privacy concerns (Figures 3 and 4) are vastly similar to the physical privacy concerns model. However, both forms of informational privacy concerns do not correlate significantly with trusting beliefs and benefits, so that H4 is partly supported.

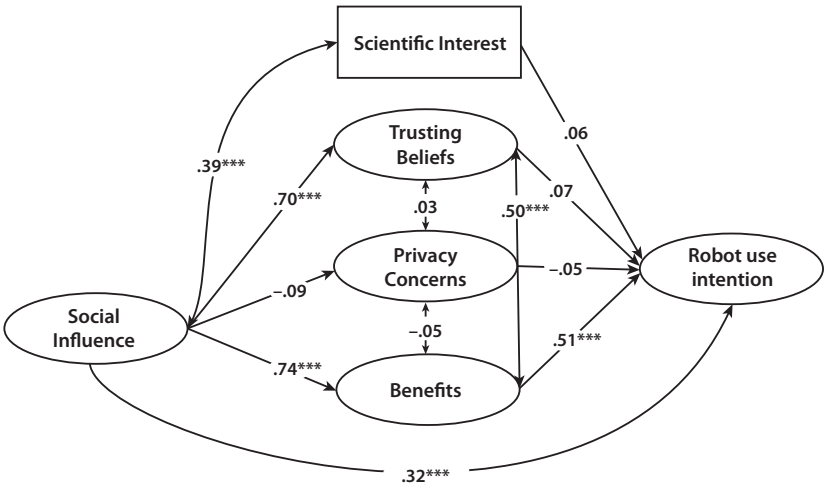

FIGURE 3 Institutional Informational Privacy Concerns Model

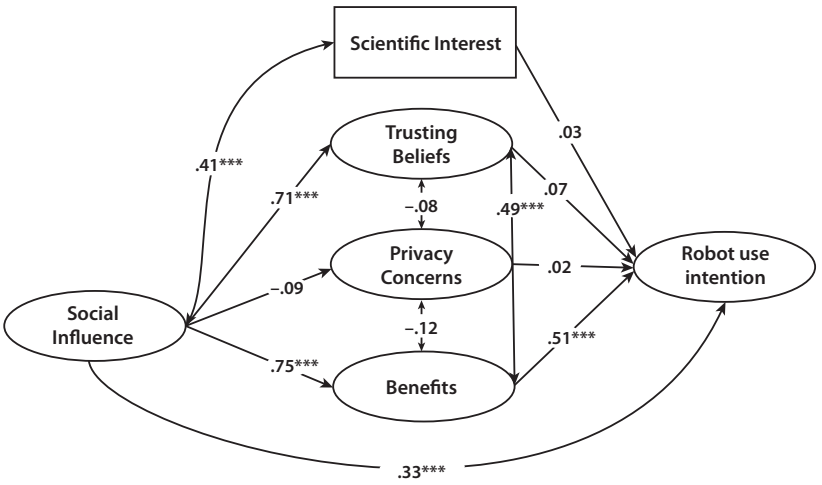

FIGURE 4 Social Informational Privacy Concerns Model

Turning to the model with global privacy concerns, we find vastly similar effects again (Figure 5), except for the role of social influence, which has the expected effect on all constructs. Therefore, H5, H6, and H8 are supported.

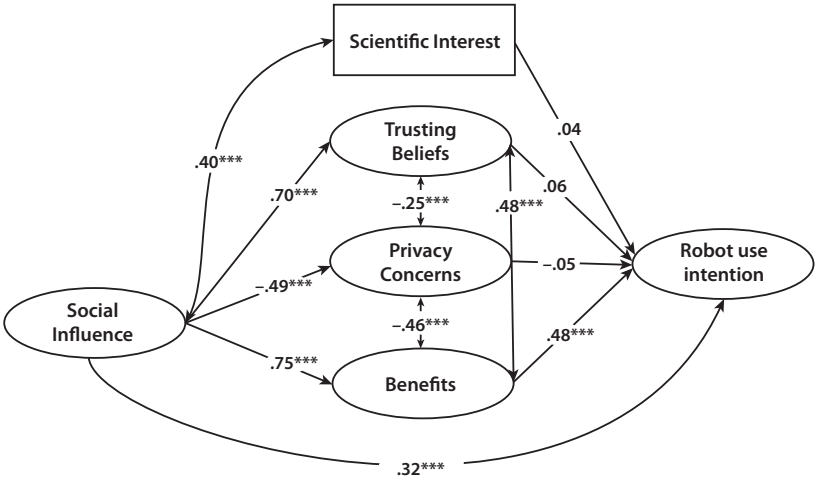

FIGURE 5 Overall Privacy Concerns Model

Across the models, we were able to explain between 72% (overall privacy concerns) and 73% (other privacy concern types) of the variance in social robot use intention. Thus, the small number of constructs has high predictive power. Particularly, the combination of perceived benefits and social influence seems to be able to predict social robot use intention strongly.

Discussion and Conclusion

Early studies on online privacy have focused on institutional privacy threats such as how service providers handle user data, especially in the domain of e-commerce (Jarvenpaa et al., 1999; McKnight et al., 2002). The emergence of social media has further intensified the debate on online privacy (Ellison et al., 2007; Krasnova et al., 2010). Accordingly, with social media, institutional privacy concerns are compounded by social privacy concerns: concerns about privacy threats that are caused by other users rather than service providers or third-party institutions (Raynes-Goldie, 2010; Young & Quan-Haase, 2013). We argue that social robots add yet another layer, with entirely new challenges to privacy, as they have mobility and thus access to private rooms (Calo, 2012).

Previous research has found a paradoxical disparity between users' privacy concerns and their online behaviors, such as a lack of privacy protection and a willingness to engage in extensive data sharing (Chen & Rea, 2004; Milne et al., 2009). Based on these findings, we developed a nomological model that considers distinct explanations for users' social robot use intention despite privacy concerns. We distinguished three types of privacy concerns and found that they were unequally pronounced. Respondents worried most about their informational privacy, especially with regard to institutions such as the social robot manufacturer. Social privacy risks, such as hacking and stalking, also evoked considerable concerns. Physical privacy concerns were less prevalent.

Perceived benefits and social influence had a significant and positive effect on social robot use intention. Some forms of privacy concerns were themselves significantly affected by social influence. This points to the explanatory value of including the social environment when looking at social robot adoption.

Our study provides a number of theoretical and practical *implications*. First, we established the existence of compounded privacy concerns in the social robot context, as we found evidence of both informational and physical privacy concerns. Second, we found a privacy paradox in line with previous studies (Kokolakis, 2017), as we detected that neither informational nor physical privacy concerns significantly affected social robot use intention. Third, we found that social dynamics are especially important in the analysis of social robot use intention. In fact, social influence drove intentions in three ways. First, it directly increased social robot use intentions; second, it reduced respondents' concerns, at least in the overall model; third and finally, it strongly increased the perceived benefits of social robots. Together, these findings demonstrate that social norms are of crucial importance in the context of social robots. As such, robot manufacturers would do well to invest in community management and they should rely heavily on word-of-mouth promotion.

As our study does not illuminate the concerns of experienced users (we sampled individuals not familiar with social robots for the most part), the implications of this research for social robot manufactures are not entirely clear-cut. Despite the apparent privacy paradox, recent media coverage of privacy issues with Internet-of-things devices, such as toys, indicates increasing public attention to these matters (Mathews, 2017). The effects of such public debate could affect the adoption of social robots as privacy concerns may influence the trust of users in the social robot manufactures and thus have an effect on the use intentions.

Thus, social robot manufacturers should be aware of the fact that consumers might value privacy and consider it in their purchasing decisions when faced with tangible risks. In that sense, manufacturers might want to increase investments into privacy-sensitive robotics (Rueben, Aroyo, et al., 2018). Not only should manufacturers develop social robots that are privacy-friendly but they should also communicate their privacy-protection efforts to potential customers in concise and transparent ways (Felzmann et al., 2019). Overall, this study highlights the compounded privacy challenges that are associated with social robots and points to its differentiated nature in affecting social robot use intention. Even if survey results on social robots and privacy concerns are bound to be abstract due to a still limited daily interaction with social robots in households, schools, or at work, empirical findings about privacy can be helpful for different stakeholders, from the academic community to practitioners and regulatory bodies.

Limitations

Our research comes with several limitations which may inspire future research on the topic. First, we conducted a cross-sectional study with a relatively low number of participants. Thus, future research should use larger and longitudinal samples, if possible representative of the whole population. Moreover, it should compare owners and users of social robots with those who are unfamiliar with them in terms of privacy concerns to investigate experience effects. Second, for the sake of brevity, our questionnaires did not assess social robots' characteristics and their perception. Future research might work with field and lab experiments and use a systematic variation of social robot characteristics to assess privacy concerns with social robots more broadly. In that regard, surveys on social robots with non-users are bound to stay relatively abstract. Thus, the results might differ from a controlled lab setting where users get to experience social robots firsthand. However, previous research has indicated that research on non-experts, such as ours, can be helpful to assess individuals' attitudes and fears of social robots, even if they have not used such technology themselves (Liang & Lee, 2017). Third, we could not assess contextual characteristics, such as users' cultural backgrounds or their social milieus. Future research could delve deeper into user characteristics and users' composition of social networks to achieve a more holistic understanding of privacy.

Acknowledgments

We would like to thank three anonymous peer reviewers of this article and the volume editor, Prof. Leopoldina Fortunati, for very helpful feedback and guidance during the peer review process.

The Research Council of Norway funded the data collection for this article as part of the first author's research funding under the Grant Agreements "247725 Fair Labor in the Digitized Economy" and "275347 Future Ways of Working in the Digital Economy."

Author Biographies

Christoph Lutz (Dr./PhD, University of St. Gallen) is an Associate Professor at the Nordic Centre for Internet and Society, BI Norwegian Business School (Oslo, Norway). His research interests include online participation, privacy, the sharing economy and social robots. Christoph has published widely in top-tier journals in this area.

https://orcid.org/0000-0003-4389-6006

Aurelia Tamò-Larrieux (Dr./PhD, University of Zurich) is a Postdoctoral Researcher at the Center for Information Technology, Society, and Law (ITSL) and Digital Society Initiative at the University of Zurich (Switzerland). Her research interests include privacy, especially privacy-by-design, data protection, social robots, and artificial intelligence. Aurelia has published widely in this area, including the book *Designing for Privacy and its Legal Framework* (Springer, 2018).

https://orcid.org/0000-0003-3404-7643

References

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Alaiad, A., & Zhou, L. (2014). The determinants of home healthcare robots adoption: An empirical investigation. *International Journal of Medical Informatics, 83*(11), 825–840. https://doi.org/10.1016/j.ijmedinf.2014.07.003

Altman, I. (1975). *The Environment and Social Behavior—Privacy, Personal Space, Territory, Crowding*. Monterey: Wadsworth Publishing Company.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday, 11*(9). https://doi.org/10.5210/fm.v11i9.1394

Bart, Y., Shankar, V., Sultan, F., & Urban, G. L. (2005). Are the drivers and role of online trust the same for all web sites and consumers? A large-scale exploratory empirical study. *Journal of Marketing, 69*(4), 133–152. https://doi.org/10.1509/jmkg.2005.69.4.133

Beldad, A., De Jong, M., & Steehouder, M. (2010). How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. *Computers in Human Behavior, 26*(5), 857–869. https://doi.org/10.1016/j.chb.2010.03.013

Bollen, K. A. (1989). *Structural equations with latent variables*. Wiley Interscience.

Butler, D. J., Huang, J., Roesner, F., & Cakmak, M. (2015). The privacy-utility tradeoff for remotely teleoperated robots. In *Proceedings of the Tenth Annual ACM/IEEE International Conference on Human-Robot Interaction* (pp. 27–34). ACM. https://doi.org/10.1145/2696454.2696484

Bygrave, L. A. (2002). *Data protection law: Approaching its rationale, logic and limits*. Wolters Kluwer.

Byrne, B. (2012). *Structural equation modeling with Mplus*. Routledge.

Calo, R. (2012). Robots and privacy. In P. Lin, G. Bekey, & K. Abney (Eds.), *Robot Ethics: The Ethical and Social Implications of Robotics* (pp. 187–202). MIT Press.

Calo, R. (2016). Robots in American law. *University of Washington School of Law Research Paper*, No. 2016-04.

Carnevale, A. (2016). Will robots know us better than we know ourselves? *Robotics and Autonomous Systems, 86*, 144–151. https://doi.org/10.1016/j.robot.2016.08.027

Chen, K., & Rea, A. I. (2004). Protecting personal information online: A survey of user privacy concerns and control techniques. *Journal of Computer Information Systems, 44*(4), 85–92. https://doi.org/10.1080/08874417.2004.11647599

Darling, K. (2016), Extending legal protection to social robots: The effects of anthropomorphism, empathy, and violent behavior toward robotic objects. In R. Calo, M. Froomkin & I. Kerr. (Eds.), *Robot Law* (pp. 213–234). Edward Elgar.

Delcker, J. (2019). *US to endorse new OECD principles on artificial intelligence*. *Politico*, May 19, 2019. Archived at https://web.archive.org/web/20190520045733/https://www.politico.eu/article/u-s-to-endorse-new-oecd-principles-on-artificial-intelligence/

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61–80. https://doi.org/10.1287/isre.1060.0080

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook 'friends': Social capital and college students' use of online social network sites. *Journal of Computer-Mediated Communication, 12*(4), 1143–1168. https://doi.org/10.1111/j.1083-6101.2007.00367.x

Eurobarometer. (2012). *Special Eurobarometer 382: Public attitudes toward robots*. http://ec.europa.eu/public_opinion/archives/ebs/ebs_382_en.pdf

Eurobarometer. (2015). *Special Eurobarometer 427: Autonomous systems*. http://ec.europa.eu/public_opinion/archives/ebs/ebs_427_en.pdf

European Commission. (2018). *Ethics guidelines for trustworthy AI: High-Level Expert Group on Artificial Intelligence*. Archived at https://web.archive.org/web/20190423110004/https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

Felzmann, H., Fosch-Villaronga, E., Lutz, C., & Tamò-Larrieux, A. (2019). Robots and Transparency: The Multiple Dimensions of Transparency in the Context of Robot Technologies. *IEEE Robotics & Automation Magazine, 26*(2), 71–78. https://doi.org/10.1109/MRA.2019.2904644

Fong, T., Nourbakhsh, I., & Dautenhahn, K. (2003). A survey of socially interactive robots. *Robotics and autonomous systems, 42*(3), 143–166. https://doi.org/10.1016/S0921-8890(02)00372-X

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39–50. https://doi.org/10.1177/002224378101800104

Gupta, S. K. (2015, 8 September). Six recent trends in robotics and their implications. *IEEE Spectrum*. Archived at https://web.archive.org/web/20190801112252/https://spectrum.ieee.org/automaton/robotics/home-robots/six-recent-trends-in-robotics-and-their-implications

Hartzog, W. (2018). *Privacy's blueprint: The battle to control the design of new technologies*. Harvard University Press.

Hoffmann, C. P., Lutz, C., & Meckel, M. (2014). Digital natives or digital immigrants? The impact of user characteristics on online trust. *Journal of Management Information Systems, 31*(3), 138–171. https://doi.org/10.1080/07421222.2014.995538

Jarvenpaa, S. L., Tractinsky, N., & Saarinen, L. (1999). Consumer trust in an Internet store. *Journal of Computer-Mediated Communication, 5*(2), 34–67. https://doi.org/10.1111/j.1083-6101.1999.tb00337.x

Kaminski, M. E. (2015). Robots in the home: What will we have agreed to? *Idaho Law Review, 51*, 661–677. Archived at https://www.uidaho.edu/-/media/UIdaho-Responsive/Files/law/law-review/articles/volume-51/51-3-kaminski-margot-e.pdf

Kaminski, M. E., Rueben, M., Grimm, C., & Smart, W. D. (2017). Averting robot eyes. *Maryland Law Review, 76*, 983–1023. https://ssrn.com/abstract=3002576

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

Koops, B. J., Newell, B. C., Timan, T., Škorvánek, I., Chokrevski, T., & Galič, M. (2016). A typology of privacy. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2754043

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology, 25*(2), 109–125. https://doi.org/10.1057/jit.2010.6

Krupp, M. M., Rueben, M., Grimm, C. M., & Smart, W. D. (2017, March). Privacy and telepresence robotics: What do non-scientists think? In *Proceedings of the Companion of the 2017 ACM/IEEE International Conference on Human-Robot Interaction* (pp. 175–176). ACM. https://doi.org/10.1145/3029798.3038384

Lee, M. K., Tang, K. P., Forlizzi, J., & Kiesler, S. (2011, March). Understanding users' perception of privacy in human-robot interaction. In *Proceedings of the 6th International Conference on Human-Robot Interaction* (pp. 181–182). ACM.

Liang, Y., & Lee, S. A. (2017). Fear of autonomous robots and artificial intelligence: Evidence from national representative data with probability sampling. *International Journal of Social Robotics, 9*(3), 379–384. https://doi.org/10.1007/s12369-017-0401-3

Lin, P. (2012). Introduction to Robot Ethics. In P. Lin, G. Bekey, & K. Abney (Eds.), *Robot Ethics: The Ethical and Social Implications of Robotics* (1st ed., pp. 3–16). MIT Press.

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

Lutz, C., & Tamò, A. (2015). RoboCode-Ethicists: Privacy-friendly robots, an ethical responsibility of engineers? In *Proceedings of the 2015 ACM Web Science Conference*, Oxford UK, 28 June–1 July 2015. ACM. https://doi.org/10.1145/2786451.2786465

Lutz, C., & Tamò, A. (2018). Communicating with robots: ANTalyzing the interaction between healthcare robots and humans with regards to privacy. In A. Guzman (Ed.), *Human-Machine Communication: Rethinking Communication, Technology, and Ourselves* (pp. 145–165). Peter Lang.

Madden, M., & Rainie, L. (2015). Americans' attitudes about privacy, security and surveillance. Pew Internet, Science & Tech Report. Archived at https://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336–355. https://doi.org/10.1287/isre.1040.0032

Mathews, L. (2017, 28 February). The latest privacy nightmare for parents: Data leaks from smart toys. *Forbes*. Archived at https://www.forbes.com/sites/leemathews/2017/02/28/cloudpets-data-leak-is-a-privacy-nightmare-for-parents-and-kids

McEachan, R. R. C., Conner, M., Taylor, N. J., & Lawton, R. J. (2011). Prospective prediction of health-related behaviours with the theory of planned behaviour: A meta-analysis. *Health Psychology Review, 5*(2), 97–144. https://doi.org/10.1080/17437199.2010.521684

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research, 13*(3), 334–359. https://doi.org/10.1287/isre.13.3.334.81

McPherson, M., Smith-Lovin, L., & Cook, J. M. (2001). Birds of a feather: Homophily in social networks. *Annual Review of Sociology, 27*(1), 415–444. https://doi.org/10.1146/annurev.soc.27.1.415

Milne, G. R., Labrecque, L. I., & Cromer, C. (2009). Toward an understanding of the online consumer's risky behavior and protection practices. *Journal of Consumer Affairs*, *43*(3), 449–473. https://doi.org/10.1111/j.1745-6606.2009.01148.x

Möllering, G. (2001). The nature of trust: From Georg Simmel to a theory of expectation, interpretation and suspension. *Sociology, 35*(2), 403–420. https://doi.org/10.1177/S0038038501000190

Netemeyer, R. G., Bearden, W. O., & Sharma, S. (2003). *Scaling procedures. Issues and applications*. Sage.

Pavlou, P. A. (2011). State of the information privacy literature: where are we now and where should we go? *MIS Quarterly, 35*(4), 977–988. https://doi.org/10.2307/41409969

Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday, 15*(1). https://doi.org/10.5210/fm.v15i1.2775

Rogers, E. (2003). *Diffusion of innovations* (4th ed.). Free Press.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review, 23*(3), 393–404. https://doi.org/10.5465/amr.1998.926617

Rueben, M., Aroyo, A. M., Lutz, C., Schmölz, J., Van Cleynenbreugel, P., Corti, A., Agrawall, S., & Smart, W. D. (2018). Themes and research directions in privacy sensitive robotics. In *2018 IEEE Workshop on Advanced Robotics and its Social Impacts (ARSO)* (pp. 1–8). IEEE. https://doi.org/10.1109/arso.2018.8625758

Rueben, M., Grimm, C. M., Bernieri, F. J., & Smart, W. D. (2017). A taxonomy of privacy constructs for privacy-sensitive robotics. *arXiv* preprint arXiv:1701.00841. https://arxiv.org/pdf/1701.00841.pdf

Sedenberg, E., Chuang, J., & Mulligan, D. (2016). Designing commercial therapeutic robots for privacy preserving systems and ethical research practices within the home. *International Journal of Social Robotics, 8*(4), 575–587. https://doi.org/10.1007/s12369-016-0362-y

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989–1016. https://doi.org/10.2307/41409970

Solove, D. J. (2008). Understanding privacy. Harvard University Press.

Stutzman, F., Capra, R., & Thompson, J. (2011). Factors mediating disclosure in social network sites. *Computers in Human Behavior, 27*(1), 590–598. https://doi.org/10.1016/j.chb.2010.10.017

Syrdal, D. S., Walters, M. L., Otero, N., Koay, K. L., & Dautenhahn, K. (2007). "He knows when you are sleeping"—Privacy and the personal robot companion. In *Proceedings of the 2007 AAAI Workshop Human Implications of Human–Robot Interaction,* Washington DC, 9–11 March 2007, pp. 28–33. AAAI. https://www.aaai.org/Papers/Workshops/2007/WS-07-07/WS07-07-006.pdf

Tamò-Larrieux, A. (2018). *Designing for Privacy and Its Legal Framework*. Springer.

Turkle, S. (2011). Authenticity in the age of digital companions. In M. Anderson & S. L. Anderson (Eds.), *Machine Ethics* (pp. 62–76). Cambridge University Press.

Van den Berg, B. (2016). Mind the air gap. In S. Gutwirth, R. Leenes, & P. De Hert (Eds.), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection* (pp. 1–24). Springer.

Venkatesh, V., & Morris, M. G. (2000). Why don't men ever stop to ask for directions? Gender, social influence, and their role in technology acceptance and usage behavior. *MIS Quarterly, 24*(1), 115–139. https://doi.org/10.2307/3250981

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425–447. https://doi.org/10.2307/30036540

Waldman, A. E. (2018). *Privacy as trust: Information privacy for an information age*. Cambridge University Press.

Warren, S. D. & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review, 4(*5), 193–220. https://doi.org/10.2307/1321160

Weiss, A., Wurhofer, D., & Tscheligi, M. (2009). "I love this dog"—children's emotional attachment to the robotic dog AIBO. *International Journal of Social Robotics, 1*(3), 243–248. https://doi.org/10.1007/s12369-009-0024-4

Westin, A. (1967). *Privacy and Freedom*. Atheneum Press.

Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook: The Internet privacy paradox revisited. *Information, Communication & Society, 16*(4), 479–500. https://doi.org/10.1080/1369118x.2013.777757

Yu, R., Hui, E., Lee, J., Poon, D., Ng, A., Sit, K., Ip, K., Yeung, F., Wong, M., Shibata, T., & Woo, J. (2015). Use of a therapeutic, socially assistive pet robot (PARO) in improving mood and stimulating social interaction and communication for people with dementia: Study protocol for a randomized controlled trial. *JMIR Research Protocols, 4*(2). https://doi.org/10.2196/resprot.4189

Appendix A
Pictures Shown To Precipitants

FIGURE A Picture of Social Robot Interacting With Teenager

https://web.archive.org/web/20200125184849/https://assets.newatlas.com/dims4/default/6ca1072/2147483647/strip/true/crop/1000x677+0+0/resize/1000x677!/quality/90/?url=https%3A%2F%2Fassets.newatlas.com%2Farchive%2Fnaonextgen-1.jpg

FIGURE B Picture of Social Robot Interacting With Woman

https://web.archive.org/web/20190705035114/https://images.theconversation.com/files/99788/original/image-20151027-4997-1oqg5sv.jpg?ixlib=rb-1.1.0&rect=868%2C800%2C4131%2C2005&q=45&auto=format&w=1356&h=668&fit=crop

FIGURE C Picture of Social Robot Interacting With Children

https://web.archive.org/web/20190704053145/https://secure.i.telegraph.co.uk/multimedia/archive/03512/pepper-1_3512887b.jpg

FIGURE D Picture of Social Robot Interacting With Senior

https://web.archive.org/web/20200125190432/https://www.knowablemagazine.org/sites/default/files/styles/750_y/public/articles/content/2017-10/Paro_Japan.jpg?itok=znt9ld_z

Appendix B
Questionnaire

Table A Questionnaire and Items Used

Trusting Beliefs (based on McKnight et al., 2002)	***Please tell us how much you agree or disagree with the following statements.***
	I believe that the robots act in my best interest.
	If I required help, robots would do their best to help me.
	Robots perform their role of offering personal services really well.
	Robots are truthful in their dealings with me.
	Robots would keep their commitments.
Social Influence (based on Venkatesh, Morris, et al., 2003)	***For the following statements, imagine you had a robot at home such as one of those shown in the pictures at the beginning of the survey. Please tell us how much you agree or disagree with the following statements.***
	People who influence my behavior think I should use such a robot.
	People who are important to me think that I should use such a robot.
	In general, my friends have supported or would support the use of such a robot.
Perceived Benefits (Eurobarometer 2012, 2015)	***Here is a list of things that could be done by robots. For each of them, please tell us using a scale from 0 to 10, how you would personally feel about it. On this scale, 0 means that you would feel totally uncomfortable and 10 means that you would feel totally comfortable with this situation. Use the slider to select the number.***
	Having a robot assist you at work. (functional)
	Having a robot do household chores. (functional)
	Having a robot assist children with their homework. (functional)
	Using a robot in school as a means of education. (functional and emotional)
	Having a robot provide services and companionship to elderly people. (emotional)
Overall Privacy Concerns (based on Malhotra et al., 2004)	***Please tell us how much you agree or disagree with the following statements.***
	Overall, I see a real threat to my privacy due to the robot.
	I fear that something unpleasant can happen to me due to the presence of the robot.
	I do not feel safe due to the presence of the robot.
	Overall, I find it risky to have such a robot.

Informational Privacy Concerns (Social and Institutional) (first three items adapted from Stutzman et al., 2011, and last four items newly developed and partly based on Malhotra et al., 2004)	***Please indicate your level of concern about the following potential privacy risks that arise when you share your personal information with a robot.***
	Other users engaging in identity theft through the robot. (social)
	Other users hacking into the robot. (social)
	Other users stalking me via the robot. (social)
	The robot manufacturer insufficiently protecting personal data. (institutional)
	The robot manufacturer tracking and analyzing personal data. (institutional)
	The robot manufacturer selling personal data to third parties. (institutional)
	The robot manufacturer sharing personal data with government agencies. (institutional)
Physical Privacy Concerns (self-developed)	***Please indicate your level of concern about the following potential privacy risks that arise when you have a robot at home.***
	The robot damaging or dirtying my personal belongings (e.g., furniture).
	The robot asking me personal questions.
	The robot snooping through my personal belongings (e.g., pictures).
	The robot entering areas that it should not access (e.g., bedroom).
	The robot using items that it should not use (e.g., bedclothes, pillows, personal hygiene products).
Scientific Interest (Eurobarometer, 2012)	***Please tell us whether you are very interested, moderately interested, or not at all interested in scientific discoveries and technological developments.***

Table note: We relied on 5-point Likert scales ranging from "strongly disagree" to "strongly agree" for all items, except for privacy concerns. Here, respondents could assess their concern on a 5-point scale ranging from "no concern at all" (1) to "very high concern" (5)."

Appendix C
Measurement Model

Table B Measurement Model

Construct	Item	Std. Loading	t-values	R^2	α	C.R.	AVE	Descriptive Statistics
Intention to use Robots (INT)	int1 int2 int3 int4	0.889 0.846 0.799 0.678	50.656*** 40.211*** 36.668*** 22.314***	0.791 0.715 0.639 0.460	0.91	0.88	0.65	Mean: 3.15 Median: 3.50 Std. deviation: 1.32
Trusting Beliefs (TRUST)	trust1 trust2 trust3 trust4 trust5	0.829 0.848 0.754 0.730 0.733	34.740*** 44.124*** 26.658*** 25.503*** 22.102***	0.687 0.719 0.568 0.533 0.537	0.89	0.89	0.61	Mean: 3.59 Median: 3.80 Std. deviation: 1.07
Social Influence (SOI)	soi1 soi2 soi3	0.658 0.632 0.821	16.272*** 15.091*** 26.657***	0.433 0.399 0.674	0.86	0.75	0.50	Mean: 2.75 Median: 3.00 Std. deviation: 1.12
Perceived Benefits (BEN)	ben1 ben2 ben3 ben4 ben5	0.747 0.761 0.808 0.749 0.812	26.874*** 29.570*** 37.284*** 26.767*** 36.409***	0.558 0.579 0.653 0.561 0.659	0.88	0.88	0.60	Mean: 7.00 Median: 6.19 Std. deviation: 3.13 (0–10 scale)
Overall Privacy Concerns (OVP)	ovp1 ovp2 ovp3 ovp4	0.736 0.790 0.882 0.936	27.445*** 29.301*** 56.349*** 79.940***	0.542 0.625 0.778 0.877	0.90	0.91	0.71	Mean: 2.61 Median: 2.25 Std. deviation: 1.19
Privacy Concerns: Social (SOP)	sop1 sop2 sop3	0.827 0.796 0.722	29.542*** 23.428*** 20.244***	0.685 0.634 0.521	0.82	0.83	0.61	Mean: 3.17 Median: 3.33 Std. deviation: 1.22
Privacy Concerns: Institutional (INP)	inp1 inp2 inp3 inp4	0.820 0.904 0.905 0.830	34.186*** 59.371*** 63.209*** 31.180***	0.672 0.818 0.820 0.688	0.92	0.92	0.75	Mean: 3.72 Median: 4.00 Std. deviation: 1.18
Physical Privacy Concerns (PHP)	php1 php2 php3 php4 php5	0.565 0.743 0.883 0.893 0.814	13.276*** 22.010*** 44.099*** 54.327*** 31.291***	0.319 0.552 0.779 0.797 0.672	0.88	0.89	0.62	Mean: 2.22 Median: 2.00 Std. deviation: 1.17
Criterion		≥ 0.5	min*	≥ 0.4, < 0.9	≥ 0.7	≥ 0.6	≥ 0.5	

α = Cronbach's Alpha; C.R. = composite reliability; AVE = average variance extracted.
Average, median, and standard deviation calculated per item and then averaged across items for each construct; N=374.

Table C Discriminant Validity Test (Fornell Larcker Criterion)

	AVE	INT	TRUST	SOI	BEN	OVP	SOP	INP	PHP
INT	0.65								
TRUST	0.61	0.43							
SOI	0.50	0.36	0.38						
BEN	0.60	0.61	0.55	0.26					
OVP	0.71	0.24	0.25	0.10	0.39				
SOP	0.61	0.01	0.01	0.01	0.02	0.21*			
INP	0.75	0.02	0.00	0.03	0.01	0.15*	0.39*		
PHP	0.62	0.01	0.04	0.00	0.04	0.24*	0.27*	0.11*	
BOP	0.60	0.06	0.01	0.05	0.01	0.02*	0.01*	0.00*	0.05*

Table note: Squared correlations between the constructs are shown; AVE = average variance extracted; * = not used in the same model; correlations between INT, TRUST, SOI, and BEN computed in the OVP model

HUMAN-MACHINE
COMMUNICATION