The Privacy Implications of Social Robots: Scoping Review and Expert Interviews

Christoph Lutz
christoph.lutz@bi.no
Nordic Centre for Internet and Society
BI Norwegian Business School
Nydalsveien 37
0484 Oslo, Norway

Maren Schöttler
maren_schoettler@web.de
Free University of Berlin
Kaiserswerther Straße 16-18
14195 Berlin, Germany

Christian Pieter Hoffmann
christian.hoffmann@uni-leipzig.de
Institute of Communication and Media Studies
University of Leipzig
Burgstraße 21
04109 Leipzig, Germany

The first author is the corresponding author.

Please cite as:

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. https://doi.org/10.1177/2050157919843961

The Privacy Implications of Social Robots: Scoping Review and Expert Interviews

Abstract

In this contribution, we investigate the privacy implications of social robots, as an emerging mobile technology. Drawing on a scoping literature review and expert interviews, we show how social robots come with privacy implications that go beyond those of established mobile technology. Social robots challenge not only users' informational privacy but also affect their physical, psychological, and social privacy due to their autonomy and potential for social bonding. These distinctive privacy challenges require study from varied theoretical perspectives, with contextual privacy and human-machine communication emerging as particularly fruitful lenses. Findings also point to an increasing focus on technological privacy solutions, complementing an evolving legal landscape as well as a strengthening of user agency and literacy.

Keywords: privacy, social robots, mobile media, scoping review, expert interviews

1 INTRODUCTION

Robotics is a rapidly advancing field. Ten years ago, Bill Gates forecast that robotics would develop as rapidly as the computer industry in the 1970s (Gates, 2008). Indeed, from 2014 to 2015, innovations in robotics almost tripled (KPMG, 2016) and companies such as Google, Amazon, and Toyota have announced sizeable investments (Gupta, 2015). Beyond industrial settings, robots are increasingly adopted in households, for example as assistants and conversation agents, and in institutions with strong emphasis on social interaction, such as hospitals, schools, and shopping centers. The demand for industrial robots is thus increasingly complemented with a demand for social robots. Social robots are embodied entities that interact with humans in some way (Fong, Nourbakhsh, & Dautenhahn, 2003). Following Bekey's (2012, p. 18) definition of a robot as "a machine, situated in the world, that senses, thinks, and acts", social robots are characterized by their physical presence, autonomy and mobility.[1] In this paper, our focus is on social robots that display human- or animal-like characteristics, such as in the cases of the humanoid robots Nao and Pepper (SoftBank Robotics, 2019a, 2019b), and the seal-like care robot Paro (PARO, 2019).

This increasingly social nature of robots has important implications for communication research and theory. Social robots, rather than serving as media through which communication between humans takes place, act as communication partners and agents themselves (Guzman, 2018). Therefore, they affect users in novel ways that differ from how more established mobile media do.

The literature has started to investigate privacy implications of social robots from several angles, stressing topics such as surveillance, black boxing, and social bonding (Calo, 2010b; Lutz & Tamò, 2015). Compared with established mobile technology, such as smartphones, robots possess increased autonomy (Bekey, 2012). In particular, social robots do

[1] Thus, we exclude software bots and virtual assistants, such as Apple's Siri, from our scope.

not need to be carried around but come with independent and enhanced mobility. This increases their potential for surveillance and access to private rooms (Calo, 2010b), which could affect users' sense of physical privacy in a negative way. However, beyond the physical dimension, we see implications for other forms of privacy as well. Robots might affect users' psychological, and social privacy (Burgoon, 1982). As human-robot interaction studies show, humans tend to ascribe human capacities to robots and anthropomorphize them (Breazeal, 2003). They can develop social bonds towards robots, with potential implications for social and informational privacy (Calo, 2010b). Finally, the issue of black boxing refers to the opacity of complex technology such as artificial intelligence and big data-driven algorithms (Pasquale, 2015). Robots increasingly rely on cloud-based data processing and a multitude of sensors and actuators, making them highly complex and intransparent systems, whose data collection is often unknown or misunderstood by users (Lee, Tang, Forlizzi, & Kiseler, 2011). Despite initial investigations into social robots, we know little about how this comparatively new form of mobile technology affects user privacy. In this paper, we will therefore address the following research question: *What are the implications of social robots for user privacy?* More specifically, we are interested in the informational, physical, social and psychological privacy implications of social robots (Burgoon, 1982; Leino-Kilpi et al., 2011).

To address the research question, we apply a mixed method approach by combining a scoping review (Pham et al., 2014) with qualitative expert interviews. In the scoping review, we analyze 33 relevant journal articles and proceedings papers, published between 2007 and 2017. The expert interviews were conducted with six leading academic and industry experts. The interviews provided depth and nuance to aspects that were underrepresented in the scoping review, for example regarding promising approaches to privacy protection. They also added a more active and personal voice to the debate around social robots and privacy. Across both studies, our findings help systematize the field of privacy-sensitive robotics. They show how

social robotics can be understood as an important field of new mobile technology that merits further attention.

2 CONCEPTS AND PREVIOUS RESEARCH

2.1 Social Robots

In line with Bekey (2012, p. 18), who conceptualizes *robots* as sensing, thinking and acting machines that are situated in the real world, Denning and colleagues (2009, p. 1) define a robot as a "cyber-physical system with sensors, actuators, and mobility". This definition highlights the mobility of robots – an attribute that distinguishes them from software-bots but places them within the field of mobile media and communication. Compared to smartphones and mobile media more generally, robots feature heightened autonomy (Smithers, 1997).

As opposed to non-social robots, *social robots* interact with people. A *social robot* can be defined as a "physically embodied, autonomous agent that communicates and interacts with humans on an emotional level" (Darling, 2012, p. 4). Thereby, social robots tend to provide psycho-social benefits that go beyond those of established mobile technology (e.g., para-social emotional bonding). To be able to naturally interact with humans, many social robots rely on sophisticated AI and collect large amounts of data, both about users and their environment. Current generations of social robots are equipped with connected sensors, cameras, rangefinders, accelerometers, and GPS-sensors (Calo, 2010b). In addition, current social robots are wireless and connected to computers or the Internet, thus being able to transmit data in real-time.

A prominent research stream in robotics, with strong ties to communication research and roots in human-computer interaction (HCI), is human-robot interaction (HRI). To situate this study, we will briefly discuss key research results from HCI and HRI on the emergence of social bonds between users and computers or robots. Communication researchers have

investigated the interaction between humans and computers under the "computers are social actors" (CASA) paradigm. Interactions with computers are generally social, even if they are not human or human-like (Nass, Steuer, & Tauber, 1994). Computers create emotional reactions, change attitudes, and affect memories. They are treated politely, perceived as colleagues, and evoke gender-stereotypes (Reeves, 2004). Particular influence on users can be achieved through the use of social and physical cues such as language and praise. Physical attractiveness can also influence user behavior (Fogg, 2002).[2]

The CASA paradigm can be applied to social robots, which often have anthropomorphic shape. Due to their appearance and behavior, social robots are particularly prone to be perceived as social actors. Turkle (2013) found that children and older adults develop emotional bonds towards toy robots. Robots are anthropomorphized by humans (Scheutz, 2012), facilitating the emergence of personal relationships. Important conditions for such relationships are the perceived autonomy of the robot and its appearance (Scheutz, 2012). Eye contact, facial expressions, and a natural voice lead to an illusion of understanding on the user side (Turkle, 2013). Despite ample research on the social bonding between humans and machines, the topic of related privacy implications is under-researched, leading to the emergence of a new field of privacy-sensitive robotics (Rueben et al. 2018).

2.2 Privacy

On a societal level, privacy is considered a fundamental right (Smith, Dinev & Xu, 2011). On an individual level, the freedom to act without surveillance is recognized as an important basis for personal self-development (Simitis, 1987) and privacy is conceptualized accordingly as a protection of liberal selfhood (Cohen, 2013; Kaminski & Witnov, 2015). It enables intellectual

[2] In terms of more general social science theories, actor-network theory (Latour, 2005; Law, 2009) has been a key voice in stressing the agency of non-human actors, including simpler objects such as keys and guns (Latour, 1994, 2000) and more complex cyber-physical systems such as healthcare robots (Lutz & Tamò, 2018).

endeavors and safeguards the social values of impartial reading, speaking, and exploring of ideas (Richards, 2013). Such a value-based understanding of privacy can be contrasted with a cognate-based understanding, where privacy is conceptualized as a state "related to the individual's mind, perceptions, and cognition rather than an absolute moral value or norm" (Smith et al., 2011, pp. 993-994). In this cognate-based understanding, which we largely follow here, privacy is tied to individuals' control of their personal space and information. Accordingly, Westin describes privacy as the "claim of individuals, groups, or institutions to determine for themselves, when, how, and to what extent information about them is communicated to others" (1968, pp. 6-7).

Empirical research has found a privacy paradox, where reported privacy concerns show little association with protection behavior (Barnes, 2006; Dienlin & Trepte, 2015; Gross & Acquisti, 2005; Kokolakis, 2017). This may be due to users willingly exchanging data access for service benefits (Dinev & Hart, 2006). Yet, some question users' ability to fully grasp privacy implications (Bartsch & Dienlin, 2016) – an aspect that may be especially salient in the context of emergent mobile technology like social robots. Obar (2015) therefore criticizes a "fallacy of data privacy self-management" as users may have neither the resources nor the faculties to effectively manage their personal data. Lyon (2001) diagnoses a "surveillance society", in which ubiquitous data collection makes citizens uncomfortable, yet they remain complicit in its pervasiveness. Dencik and Cable (2017) propose the concept of "surveillance realism" to describe user resignation towards seemingly unavoidable breaches of privacy. Similarly, Hargittai and Marwick (2016) describe the phenomenon of "privacy apathy" and Hoffmann, Lutz and Ranzini (2016) identify "privacy cynicism" among users of digital services.

The distinction between public and private spaces is particularly relevant for the discussion of privacy. The physical world is increasingly permeated by virtual elements, which

leads to a fuzziness when separating private and public spaces (Rouvroy, 2008). This blurring of boundaries becomes apparent with the Internet-of-things and with autonomous vehicles (Acharya, 2015). It also applies to social robots, which, due to their mobility, can access private areas, such as bedroom and bathrooms, more easily than other technology (Calo, 2010b). This, in turn, increases the complexity of the privacy challenges associated with the technology. Leino-Kilpi et al. (2001), based on Burgoon (1982), differentiate the following four dimensions of privacy:

- physical privacy: personal space and territory
- psychological privacy: values and thoughts
- social privacy: social contacts and influence
- informational privacy: personal information.

This typology serves as the basis for our paper. The typology was chosen because it offers a more inclusive perspective than other frameworks, such as the widely used distinction between informational and physical perspective (Smith et al., 2011). At the same time, it is relatively intuitive to understand and applicable to emerging technology such as social robots. In the context of social robots, the dimensions of *psychological* and *social privacy* correspond with the social bonding and boundary management processes between robots and humans. The dimension of *physical privacy* is affected by the physical nature and mobility of social robots, while social robots' data collection and processing capacities influence users' *informational privacy*. While informational privacy is the dominant dimension discussed in current privacy research, the literature occasionally delves into other dimensions of privacy, too (e.g., Lutz, Hoffmann, Bucher, & Fieseler, 2018).

3 METHODS

3.1 Scoping Review

To systematically assess the published research on the privacy implications of social robots, we conducted a scoping (literature) review. A scoping review is similar to a systematic literature review[3], for example in its systematic assessment of the literature, but with some important differences (Arksey & O'Malley, 2005; Pham et al., 2014). Scoping reviews address broader topics, whereas systematic literature reviews are more narrow in scope and have a specific research question. Scoping reviews address a broader variety of methodological approaches and research designs, whereas systematic literature reviews often focus on one specific study design such as randomized control trials. Finally, scoping reviews are more descriptive, putting less emphasis on the quality evaluation of included studies. Systematic literature reviews, by contrast, critically review the quality of the research, including aspects such as risk and bias (Pham et al., 2014). Our scoping review was conducted using the five steps of the Cochrane Reviews (Khan, Kunz, Kleijnen, & Antes, 2003, see also Levac, Colquhoun, & O'Brien, 2010, for the steps of a scoping review): the development of a research question, a systematic literature search, a quality evaluation of the identified studies, a quantitative data synthesis, and an interpretation of the results.

Web of Science was used as the literature database, where our search was limited to peer-reviewed publications. Search terms were entered as "Topic" to generate as many search results as possible. The following search terms were used: *privacy* AND (*robots* OR *robotics*). The search was performed in July 2017. The combination of *robot* and *privacy* returned 46 results. The combination of *robotics* and *privacy* resulted in 31 search hits. Of the 77 search

[3] A common definition of a systematic literature review is a "transparent procedure to find, evaluate and synthesize the results of relevant research" (Campbell Collaboration, 2017). In the social sciences, systematic literature reviews serve to examine and evaluate existing research with regard to a specific question (Oakley, Gough, Oliver, & Thomas, 2005), and to aggregate a state of knowledge across disciplines (Feak & Swales, 2011).

results, 17 duplicates were removed, leaving 60 results. These were examined based on relevance, availability, and language. The relevance of the publications was determined on the basis of their abstract, and, based on this criterion, a further 35 publications were excluded. The criterion of relevance refers to whether both robots *and* privacy were the focus of the paper and whether both topics were related to each other. Moreover, the paper had to address *social* robots specifically. Thus, this criterion was used to exclude papers that focused on either robots *or* privacy with no significant reference to the other topic. For instance, papers that focused on technical experiments with robots and barely touched upon the issue of privacy were excluded. Three further publications were unavailable. A publication published in Swedish was ruled out on the basis of language. This resulted in a relatively small body of research (n=21) corresponding with the recency of the research field. To ensure a comprehensive overview, 12 further publications were included in a theory-based literature search. These were identified through an analysis of citations within the publications identified in the systematic search. This results in a corpus of 33 salient studies. The papers were then coded by hand. The publications examined are marked with * in the bibliography of this work. Publications included in the literature review but not explicitly cited in the text are listed in the Appendix.[4]

3.2 Expert Interviews

In addition to the scoping review, we conducted semi-structured expert interviews to further address the research question. This mixed method approach was based on a convergent parallel design (Creswell & Plano Clark, 2017). Expert interviews were chosen to complement and contextualize the findings from the scoping review, as the analyzed observable research field

[4] Following a reviewer suggestion, we repeated the literature search in the article revisions process with the same time window as before but including wildcard operators. We used robot* instead of (robots OR robotics) and queried Scopus in addition to Web of Science. This resulted in a larger pool of results: 173 publications for Web of Science and 596 for Scopus. After checking each entry for relevance and previous inclusion, we found four additional publications that are listed in the Appendix.

is still very recent and further context could be needed to understand its current structure, foci as well as gaps, and potential further development. The expert interviews were pre-structured by an interview guideline of 23 questions (see Appendix) and addressed topics such as personal experience with robots, social robots' effects on user privacy, privacy protection behavior, and solutions to privacy challenges. The guideline was designed to cover a wide range of topics that lend themselves to privacy research, allowing for interaction during the interpretation of the scoping review. The latter was itself set up to capture an overview of the field.

For the purposes of this study, we defined experts as individuals who deal with the privacy implications of social robots, either as an academic or in practice (i.e., in a company that develops social robots). The selection of academic experts was influenced by the scoping review and the experts were selected on the basis of three criteria: the possession of relevant information, the ability to pass on precise information, and availability (Table 1). All interviews were conducted between June 27 and August 16 2017 by either phone or Skype call, recorded, and transcribed. The interview duration averaged around 30 minutes.

Data collection for the scoping review and expert interviews was conducted concurrently and largely independently, with the exception of the choice of academic experts for the interviews. Both strands of research were then combined during data analysis and, primarily, interpretation (Creswell & Plano Clark, 2017). Findings from the scoping review were cross-referenced, triangulated and contextualized with expert observations to gain a deeper understanding of the development of the theoretical discourse, emergent foci, research gaps, and congruence or potential discrepancies with observations from practice.

INSERT TABLE 1 HERE

4 RESULTS

4.1 Scoping Review: Quantitative Data Synthesis

All publications in the literature review were published between 2007 and 2017, the vast majority of them in scientific journals or conference proceedings (n=30). Studies are distributed across different outlets, with three publications in *Ethics and Information Technology*, and two each in *Connection Science*, *Interaction Studies*, *Human Robot Interaction*, and *Computer Law & Security Review*.

Since 2008, we observe a slowly rising interest in the topic (Figure 1). There is an uptick in published studies per year after 2015, which may indicate a further expansion of the field. However, to date, the annual publication rate is low.

INSRT FIGURE 1 HERE

The identified studies are situated mainly in law (25.6%), computer science (20.5%), medicine and health sciences (15.4%). Other research disciplines represented are information systems (10.3%), psychology (10.3%), political science (7.7%), and robotics (5.1%). Media and communication as well as philosophy are each represented by one publication (2.6%, see Table 2). Some publications were counted twice, as they were created as collaborations between researchers from different disciplines. Altogether, seven of the 33 publications are the result of interdisciplinary cooperation (21.2%).

INSERT TABLE 2 HERE

The majority of publications feature a conceptual or critical approach (72.7%), with only nine empirical studies (27.3%). Robots used in the care sector (30.3%), especially in geriatric care (21.2%), attract most attention. Social robots for children were investigated in two publications (6.1%) and social robots for teaching in one (3%).

The identified publications differ in their understanding of privacy. The majority are concerned with informational privacy. However, some authors do not refer to any definition or typology of privacy (e.g., Lee et al., 2011). This is particularly common when privacy is discussed as an aspect of ethical concerns, where an understanding of privacy as informational privacy is often implied.

Table 3 provides an overview of the empirical studies within the corpus. Most frequently, they examined groups of elderly people (33.3%) and nursing staff (25%). In addition, potential end users (Zsiga, Edelmayer, Rumeau, Péter, Tóth, & Fazekas, 2013), adults (Lee et al., 2011), parents (McReynolds et al., 2017) and university staff (Syrdal, Walters, Otero, Koay, & Dautenhahn, 2007) were investigated in one study each.

INSERT TABLE 3 HERE

Qualitative methods were used in seven studies (77.8%), while two applied both qualitative and quantitative methods (22.2%). Focus groups, surveys, and interviews were each applied in two studies. Only one study was based on an experimental design (Denning et al., 2009). A combined methodology of survey, interview and observation was used in another study (Caine, Šabanović, & Carter, 2012). Thus, qualitative methods are currently the preferred approach in the research field.

Among the identified empirical studies, four focus on household robots and nursing robots (44.4%) while one analyzes toy robots (11.1%). However, some studies do not use real social robots, but merely show the research subjects videos or explain how they work (cf. Draper & Sorell, 2017; Lee et al., 2011). Some areas of application addressed in conceptual articles, such as childcare or teaching tasks (Sharkey, 2016; Sharkey & Sharkey, 2010), are not represented in the empirical studies. Overall, the empirical body of knowledge is quite thin and disparate.

4.2 Scoping Review and Expert Interviews: Interpretation of the Results

Theories and concepts. Due to their varied disciplinary backgrounds, the identified studies apply a range of theories and models, but two main concepts tend to exert a notable influence on the field: *"privacy as contextual integrity"* (Nissenbaum, 2004) and *"fair information practices"* (Sedenberg, Chuang, & Mulligan, 2016). The theory of privacy as contextual integrity emphasizes the need to consider the transfer of personal information contextually, depending on the situation and its social norms (Nissenbaum, 2004). This theory is addressed in several conceptual articles (Fosch Villaronga & Roig, 2017; Lutz & Tamò, 2015; Pagallo, 2013; Sedenberg et al., 2016). In contrast, fair information practices focus on the right of individuals to protect their privacy through informed and self-determined action. This concept is the dominant approach for the protection of informational privacy (Sedenberg et al., 2016). However, given the difficulty of establishing informed consent with social robots, its applicability was questioned by the interviewed experts. One expert encouraged a movement away from notice and consent towards "visceral notice" and nudges through technology, for example *"having a visual cue that the robot, the toy is recording. And providing more clear information visually that this is happening"* (Expert 6).

Research on privacy in HRI tends to examine one dimension of the privacy concept in isolation (Rueben, Grimm, Bernieri, & Smart, 2017). Referring back to the typology of privacy presented earlier (Burgoon, 1982; Leino-Kilpi et al., 2001), it is noticeable that privacy is often reduced to informational privacy. Other aspects such as physical privacy are rarely taken into account. However, social robots tend to affect multiple dimensions of privacy. For example, violations of physical or psychological privacy by social robots are possible to an extent that is not the case with other technologies. *"Over the years the definition of privacy has kind of evolved. It began with privacy, at least informational privacy, having something to do with control over personal information. That definition is no longer adequate if it ever was. […]*

And so now I think of privacy as being largely about the role of autonomy in a world that is so data-promiscuous" (Expert 4).

Privacy threats. Users' *informational privacy* is endangered by the increased capacity of social robots for data collection. Social robots collect information about the everyday life of users (Calo, 2010b) and, through numerous sensors, they increasingly collect information about sensitive characteristics such as emotional and mental states (Lee, et al., 2011; Sedenberg et al., 2016; Sharkey, 2016). For example, users casually commenting on their personal feelings when interacting with a robot allow for the recording of previously difficult to gage information. Sensitive information also includes images of users in bedrooms and bathrooms, for example as users undress with their robot present (Sharkey & Sharkey, 2012b), information about the floor plan in their homes, and information about diseases, dependencies, health conditions or disabilities (Syrdal et al., 2007). A study by Syrdal et al (2007) notes that information about the personality of users is considered particularly sensitive and that users feel uncomfortable when such information is collected.

In addition, social robots can detect more than what users can perceive, for example by detecting electromagnetic forces or changes in brain waves (Calo, 2010a). Robots can also detect places that are inaccessible to users (Rueben et al., 2017). Thereby, robots may "know" more about the living conditions (e.g., health risks) of their users than the users themselves. The fact that social robots collect more sensitive data than previous mobile technologies is therefore highlighted in many publications and was recognized across different interviews. One expert made the example of a robot used in elderly care that could detect whether a person had fallen: "*Now, I think falling is really an extremely important case. Because if elderly people fall, that is often taken to be a reason for putting them in a care home.* […] *So, there is a case where these people had access to information about the falls of a particular person. That*

person might in a sense lose their freedom. And so in such a case, it is important that the person themselves be able to control whether that information reaches somebody else." (Expert 5).

Furthermore, cloud storage of data collected by social robots is considered problematic (Pagallo, 2013), as is the connectivity of social robots with the Internet and among each other (Sedenberg et al., 2016; Sharkey, 2016). This leads to a higher susceptibility to hacking. An experimental study confirms this risk potential and found that household robots could simply be infiltrated by outsiders and without direct contact with the robots (Denning et al., 2009). In other words, through social robots, hackers may gain much deeper insights into the lives of their victims than, for example, through laptops or tablets. While most experts recognized that social robots may become the target of hacking (Experts 2, 3, and 4), some advocating for using social robots of larger companies, which offer better security than smaller startup companies, a minority suggested that the interest in hacking may be low due to low adoption at this point (Experts 5 and 6). Expert 5 presented such a dissenting view: *"You know, another question is whether robots would be the targets of people who are interested in hacking. And my sense would be that they are not. […] So I am not sure it is a big issue in relation to robots but it's certainly an issue"*.

Social robots are a novel technology whose functions remain little understood by the majority of users (Lutz & Tamò, 2015). Several studies point out how users lack awareness and do not understand the collection of data by social robots (Caine et al., 2012; Draper & Sorell, 2017; Lee et al., 2011). Demographic differences were found, especially in terms of age, where younger caregivers were more concerned about privacy and safety than older caregivers, who, in turn, were more interested in functionality and emotional companionship (Zsiga et al., 2013). Thereby, the concept of the "privacy-utility tradeoff" applies to social robots: The acceptance of data collection depends on the usefulness of the robot and the sensitivity of the data (Syrdal et al., 2007). This is especially relevant given social robots'

unique socio-psychological and emotional benefits, which may lead to more privacy lenience among users. Some point out that informed consent to continuous data collection and monitoring by social robots is not possible (Draper & Sorell, 2017). Conceptual studies also raise concerns about access to collected information by third parties that users may not be aware of as they focus on their particular robot (Fosch Villaronga & Roig, 2017; Hofmann, 2013; Kaminski, 2015; Sharkey, 2016).

The *social* dimension of social robots plays a key role in data collection: Through their social character and interactivity, social robots collect more sensitive information (Pagallo, 2013), particularly in cases of emotional relationships between user and social robot (Calo, 2011). By developing affection and trust, secrets can be revealed (Lee et al., 2011; Sharkey, 2016). Expert 3 elaborates on this point: *"I mean there have been studies with this robot that in the home, I think it was the Adam robot made by MIT, where people would be very happy to tell it all of their worries because there wasn't an actual, a real social agent, it wasn't a friend or a colleague, it was a robot. And so they were able to speak to it and tell them all of their worries even more so than they would with real people."* As a result, social robots affect users' *social* and *psychological privacy*. For example, social robots may record data on the intimacy of interaction with the user or personal thoughts uttered to a robot like to a present human being.

On the other hand, the literature review and the experts highlighted that a sense of surveillance and access to private spaces can lead to a change in users' social behavior, leading to less information disclosure (Calo, 2011). For example, it is argued that the feeling of being alone may be prevented by social robots, which leads to reduced self-development and self-reflection (Calo, 2011; Sedenberg et al., 2016). The *psychological* effects such as conformity and loss of freedom are also discussed in the literature (Calo, 2010b; Calo, 2011; Kaminski, 2015). The presence of social robots may change users' attitudes and behaviors (Calo, 2010b).

The protection of privacy for identity development and the development of healthy relationships based on trust may be inhibited by the continuous presence and "always on mode" of the social robot (Broadbent, 2017). In children, for example, developmental problems are feared, such as the creation of insecure attachments to robots that extend to interpersonal attachments (Sharkey & Sharkey, 2010). However, to date, many of these critical perspectives are put forth in conceptual studies and there is a lack of empirical evidence on the consequences of surveillance and privacy infringements. Still, these critical perspectives are addressing important concerns that might further emerge in the future. For instance, they point towards potential psychological effects on users and therefore provide a basis for future research to test the generated hypotheses empirically.

Finally, the *physical privacy* of users can be affected by social robots – despite comparatively little discussion of this in the studied literature. The mobility and physicality of social robots create the potential to harm users and their environment due to their mobility and autonomy (Calo, 2015). In other words, as opposed to mobile phones or smart speakers, social robots tend to be mobile and have access to private spaces such as bedrooms or bathrooms (Calo, 2011), they can collect spatial information or witness conversations largely unnoticed by the user if they enter a space at an inconvenient time. Connected to aspects of social and psychological privacy, the presence of robots changes the home as a place of security, privacy, and security, and negatively influences the character of private spaces as places of retreat (Sedenberg et al., 2016). As a result, users feel insecure and alienated (Hofmann, 2013). Expert 1 describes aspects of physical privacy: *"They can do a lot of the things that humans can. Like, they can get too close just like the human can get too close. They can make you feel uncomfortable, things like that."*

At the same time, the majority of empirical studies show both a high acceptance of social robots as well as few concerns about privacy intrusions on the user side (Draper & Sorell,

2017; Sadasivam et al., 2014; Zsiga et al., 2013). Nevertheless, certain privacy concerns have been identified (Syrdal et al., 2007; Zsiga et al., 2013). Parents, in particular, are concerned about social robots as toys (McReynolds et al., 2017).

INSERT TABLE 4 HERE

Privacy protection. A technological solution to privacy threats identified in the literature is the concept of "*privacy by design*" (Calo, 2011; Lutz & Tamò, 2015; Sanfeliu, Llácer, Gramunt, Punsola & Yoshimura, 2010). Here, privacy protection is taken into account from the very beginning of the development process of a social robot (Carnevale, 2016). However, the "privacy by design" concept is not considered to be effective in all the publications examined. Since social robots are primarily shaped by their users, such pre-programming is not deemed sufficient. Therefore, aside from regulators, designers or manufacturers, users themselves are responsible and required to protect their privacy (Pagallo, 2013). After all, the jurisdiction tends to lose its effectiveness in private spaces (Schafer & Edwards, 2017). The experts largely agreed that technological aspects play a promising role in protecting user privacy. Technological privacy solutions mentioned include being able to switch off a robot (Expert 4), limiting its movement space (Expert 1), data anonymization (Experts 2), and designing a robot's eyes and ears in a way to signal that data is being collected (Experts 1, 3, 6). Regarding the latter, a study compared surveillance cameras, a stationary, and a mobile robot in terms of privacy protection. Contrary to expectations, most privacy enhancing behaviors (PEBs) were observed in interactions with surveillance cameras, but not with the robots (Caine et al., 2012). The anthropomorphic shape of the robot disguised the possibility of data collection (Caine et al., 2012; Lee et al., 2011). Finally, an opportunity is also seen in

replacing written terms of use with verbal communication with the social robot (Calo, 2010a; Lee et al., 2011; Lutz & Tamò, 2015).

For the protection of informational privacy, *transparency* and *control* over personal data are mentioned (Sedenberg et al., 2016). Calo (2010) points out, however, that known mechanisms for data protection such as encryption and anonymization are no longer sufficient, as they are not able to capture the specific interventions in the physical and psychological privacy of the user. This discussion is seen as an opportunity for an understanding of privacy that goes beyond informational privacy. Such an updated understanding should be based on users and their technology experiences (Calo, 2010a), so that the protection of informational privacy should be linked to the functions and roles of the social robot (Pagallo, 2013). The experts proposed different methods for raising user awareness, from extensive discussions about privacy and education on the subject in schools, on television, and through advertising messages, to interpersonal communication and the exchange of personal experiences (Expert 1).

US scholars criticize the existence of legal grey areas and the unequal distribution of power in favor of the state and companies against users (Calo, 2011; Calo, 2015; Kaminski, 2015). They call for a strengthening of user rights (Calo, 2011) and an adaptation of the legal framework for new technologies. Data protection laws should be further developed with regard to special features and novel threats from social robots (Calo, 2015). The experts discussed principles such as purpose limitation and data minimization (Experts 1), particularly in the context of the GDPR (Expert 6). *"The legal means are there, they just have to be implemented consistently"* (Expert 2).

5 DISCUSSION AND CONCLUSION

The goal of this paper, by providing a contextualized review of the state of research, was to investigate the privacy implications of social robots. Specifically, we intended to show how social robots present differentiated privacy risks that go beyond those of established mobile technology such as smartphones. Through the scoping review, we provided an overview of a young, but deeply interdisciplinary research field. We found that conceptual and critical articles are more prevalent than empirical studies. To date, empirical studies mostly rely on small sample sizes and their results are not representative and generalizable. These studies also only look at certain aspects of privacy, mostly informational privacy. The application areas of social robots are strongly differentiated and are investigated independently, which further reduces the comparability and generalizability of the empirical findings.

The conceptual and critical articles mostly deal with the question of the distinctive qualities of social robots, as opposed to other technologies – and the specific challenges associated with these qualities. The most important feature mentioned here was their social character. Robots as mobile, autonomous and naturalized actors collect more sensitive information and threaten privacy in novel ways. For example, through verbal communication with the robot (some of it spontaneous and informal), sensitive information is produced. Also the physical embodiment and mobility of social robots enable the collection of sensitive data from areas in which users do not intend to be observed. These issues are exacerbated if data processing happens in the cloud, as data collected in intimate settings is transmitted, analyzed and stored beyond the users' control.

The psychological influence of social robots is particularly high as users may create emotional bonds with their robots and interact with them in a more open, intimate way. From a privacy calculus perspective, social robots may offer new social and emotional benefits that would render users willing to share more intimate data (Dinev & Hart, 2006). At the same time,

from a privacy literacy standpoint, it is questionable if users are capable of grasping the privacy ramifications of this new technology and give informed consent to data collection (Bartsch & Dienlin, 2016; Obar, 2015). Some authors warn that social robots introduce new elements of surveillance, which might lead to conformity and a lack of self-reflection (Calo, 2010b; Calo, 2011; Kaminski, 2015). On the other hand, with the proliferation of social robots, recent phenomena such as "surveillance realism" (Dencik & Cable, 2017), "privacy apathy" (Hargittai & Marwick, 2016), or "privacy cynicism" (Hoffmann et al., 2016) may become more pronounced as users become ever more reliant on ever more complex technology with difficult to manage, complex privacy ramifications.

Our analysis highlights that the privacy implications of social robots go beyond informational privacy. Despite privacy risks in other dimensions, however, the majority of potential issues, both in the scoping review and in the expert interviews, were connected to informational privacy. As the experts noticed, informational privacy is the privacy dimension which is currently most covered through legal frameworks. However, intrusions into users' physical, social, and psychological privacy pose new challenges. It is particularly problematic that social and psychological implications are hard to assess and prevent. Currently, the primary responsibility for protecting their social and psychological privacy rests with the users themselves (Obar, 2015). Therefore, the interviewed experts point to several technological propositions to sensitize users.

Privacy by design and privacy as contextual integrity (Nissenbaum, 2004) emerged as dominant conceptual lenses, both in the scoping review and the expert interviews. However, privacy by design was in some instances considered to be ineffective as learning technologies might adapt through user interaction, thus rendering initial privacy implementations impractical or obsolete. Emerging literature in human-machine communication (Guzman, 2018; Lutz & Tamò, 2018) could help theorize social robots in terms of their mediality and

communicative affordances. This would be useful for the design of empirical studies on the privacy implications of social robots. Such studies could adopt ethnographic and novel user-centered methods (e.g., Light, Burgess, & Duguay, 2018), considering how the materiality and design of the technology interact with user expectations and practices as well as the wider social context (Beane & Orliwokski, 2015). Suchman's (2007) work on human-machine configurations, the social construction of technology approach (Pinch & Bijker, 1984) and related scholarship in science and technology studies could inspire research on boundary management when users interact with social robots. An important question in that regard is whether social robots can not only endanger users' privacy but potentially preserve or even enhance it. Finally, future research could differentiate individual privacy types further. Particularly within the area of informational privacy, the distinction between social and institutional privacy concerns (Raynes-Goldie, 2010; Young & Quan-Haase, 2013) can be used to measure users' privacy risk perception of different stakeholders (e.g., manufacturer, hackers, other users, third-party software providers) across settings.

Technological solutions, including anonymization, encryption, the possibility to switch off a robot, and design that signals data collection were seen as the most promising solutions, both in the literature review and in the expert interviews. Another central recommendation was the call for increased interdisciplinarity, spanning psychology, design, technology, communication, and law. Such an interdisciplinary approach requires a comprehensive understanding of the privacy concept, covering more than just informational privacy.

REFERENCES

Acharya, A. (2015). Are we ready for driver-less vehicles? Security vs. privacy - A social perspective. *arXiv:1412.5207v1*

*Alaiad, A., & Zhou, L. (2014). The determinants of home healthcare robots adoption. *International Journal of Medical Informatics, 83*(11), 825-840.

Arksey, H., & O'Malley, L. (2005). Scoping studies: towards a methodological framework. *International Journal of Social Research Methodology, 8*(1), 19-32.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday 11*(9).

Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior, 56*, 147-154.

Beane, M., & Orlikowski, W. (2015). What difference does a robot make? The material enactment of distributed coordination. *Organization Science, 26*(6), 1553-1573.

Bekey, G. (2012). Current trends in robotics: Technology and ethics. In P. Lin, K. Abney & G. A. Bekey (Eds.), *Robot Ethics: The Ethical and Social Implications of Robotics* (pp. 17-34). Cambridge: The MIT Press.

Breazeal, C. (2003). Toward sociable robots. *Robotics and Autonomous Systems, 42*(3-4), 167-175.

*Broadbent, E. (2017). Interactions with robots: The truth we reveal about ourselves. *Annual Review of Psychology, 68*, 627-652.

Burgoon, J. (1982). Privacy and communication. In M. Burgoon (Ed.), *Communication Yearbook* 6 (pp. 206-249). Beverly Hills, CA: Sage.

*Caine, K., Šabanović, S., & Carter, M. (2012). The effect of monitoring by cameras and robots on privacy enhancing behaviors of older adults. In *Proceedings of the Seventh Annual ACM/IEEE International Conference on Human-Robot Interaction*, 343-350.

*Calo, R. (2010a). People can be so fake: A new dimension to privacy and technology scholarship. *Penn State Law Review, 114*(3).

*Calo, R. (2010b). Robots and privacy. In P. Lin, K. Abney & G. A. Bekey (Eds.), *Robot Ethics: The Ethical and Social Implications of Robotics* (pp. 187-201). Cambridge: The MIT Press.

*Calo, R. (2011). Peeping Hals. *Artificial Intelligence, 175*(5-6), 940-941.

*Calo, R. (2015). Robotics and the lessons of cyberlaw. *California Law Review, 103*(3), 513-563.

Campbell Collaboration (2017). *What is a systematic review?* Retrieved from https://www.campbellcollaboration.org/research-resources/writing-a-campbell-systematic-review/systemic-review.html

*Carnevale, A. (2016). Will robots know us better than we know ourselves? *Robotics and Autonomous Systems, 86,* 144-151.

Cohen, J. (2013). What privacy is for. *Harvard Law Review, 126,* 1904-1933.

Creswell, J. W., & Plano Clark, V. L. (2017). *Designing and conducting mixed methods research*. Thousand Oaks, CA: Sage.

Darling, K. (2012). Extending legal rights to social robots. *SSRN Electronic Journal*, 1-13. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2044797

Dencik, L., & Cable, J. (2017). The advent of surveillance realism: Public opinion and activist responses to the Snowden leaks. *International Journal of Communication, 11,* 763-781.

*Denning, T., Matuszek, C., Koscher, K., Smith, J., & Kohno, T. (2009). A spotlight on security and privacy risks with future household robots. In *Proceedings of the 11th International Conference On Ubiquitous Computing*, 105-114.

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology,* 45(3), 285-297.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), 61-80.

*Draper, H., & Sorell, T. (2017) Ethical values and social care robots for older people. *Ethics and Information Technology, 19*, 49-68.

Feak, C., & Swales, J. (2011). *Telling a research story: Writing a literature review*. Ann Arbor, MI: University of Michigan Press.

Fogg, B. J. (2002). Persuasive technology: Using computers to change what we think and do. *Ubiquity, December*, Article No. 5.

Fong, T., Nourbakhsh, I., & Dautenhahn, K. (2003). A survey of socially interactive robots. *Robotics and Autonomous Systems, 42*(3-4), 143-166.

*Fosch Villaronga, E., & Roig, A. (2017). European regulatory framework for person carrier robots. *Computer Law & Security Review, 33*, 502-520.

Gates, B. (2008). A robot in every home. *Scientific American, 18*, 4-11.

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM workshop on Privacy in the Electronic Society* (pp. 71-80). New York: ACM.

Gupta, S. (2015). Six recent trends in robotics and their implications. *IEEE Spectrum*. Retrieved from http://spectrum.ieee.org/automaton/robotics/home-robots/six-recent-trends-in-robotics-and-their-implications

Guzman, A. (2018). Introduction: What is human-machine communication, anyway? In A. Guzman (Ed.), *Human-Machine Communication: Rethinking Communication, Technology, and Ourselves* (pp. 1-28). Bern: Peter Lang.

Hargittai, E., & Marwick, A. (2016). "What can I really do?" Explaining the privacy paradox with online apathy. *International Journal of Communication, 10*, 3737-3757.

Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 10*(4), article 7.

*Hofmann, B. (2013). Ethical challenges with welfare technology. *Science Engineering Ethics, 19*(2), 389-406.

*Kaminski, M. (2015). Regulating real-world surveillance. *Washington Law Review, 113*(9), 1113- 1165.

Kaminski, M., & Witnov, S. (2015). The conforming effect: First Amendment implications of surveillance, Beyond Chilling Speech. *University of Richmond Law Review, 49*, 483-493.

Khan, K., Kunz, R., Kleijnen, J., & Antes, G. (2003). Five steps to conducting a systematic review. *Journal of the Royal Society of Medicine, 96*(3), 118-121.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64*, 122-134.

KPMG (2016). *Social robots*. KPMG Advisory. Retrieved from https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/social-robots.pdf

Latour, B. (1994). On technical mediation—philosophy, sociology, genealogy. *Common Knowledge, 3*(2), 29–64.

Latour, B. (2000). The Berlin Key or how to do words with things. In P. M. Graves-Brown (Ed.), *Matter, Materiality, and Modern Culture* (pp. 10–21). London: Routledge.

Latour, B. (2005). *Reassembling the social. An introduction to actor-network-theory*. Oxford: Oxford University Press.

Law, J. (2009). Actor network theory and material semiotics. In B. S. Turner (Ed.), *The New Blackwell Companion to Social Theory* (pp. 141–158). Hoboken, NJ: Wiley.

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

Leino-Kilpi, H., Välimäki, M., Dassen, T., Gasull, M., Lemonidou, C., … & Arndt, M. (2001). Privacy: A review of the literature. *International Journal of Nursing Studies, 38,* 663-671.

Levac, D., Colquhoun, H., & O'Brien, K. K. (2010). Scoping studies: advancing the methodology. *Implementation Science, 5*(1), 69.

Light, B., Burgess, J., & Duguay, S. (2018). The walkthrough method: An approach to the study of apps. *New Media & Society, 20*(3), 881-900.

Lutz, C., Hoffmann, C., Bucher, E., & Fieseler, C. (2018). The role of privacy concerns in the sharing economy. *Information, Communication & Society, 21*(10), 1472-1492.

*Lutz, C., & Tamò, A. (2015). RoboCode-Ethicists - Privacy-friendly robots, an ethical responsibility of engineers? In *Proceedings of the 2015 ACM Web Science Conference*.

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). Bern: Peter Lang.

Lyon, D. (2001), *Surveillance society: Monitoring everyday life*. Philadelphia, PA: Open University Press.

*McReynolds, E., Hubbard, S., Lau, T., Saraf, A., Cakmak, M., & Roesner, F. (2017). Toys that listen: A study of parents, children, and Internet-connected toys. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 5197-5207.

Nass, C., Steuer, J., & Tauber, E. R. (1994). Computer are social actors. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 72-78.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review, 79,* 101-139.

Oakley, A., Gough, D., Oliver, S., & Thomas, J. (2005). The politics of evidence and methodology: lessons from the EPPI-Centre. *Evidence & Policy: A Journal of Research, 1*(1), 5-32.

Obar, J. A. (2015). Big data and the phantom public: Walter Lippmann and the fallacy of data privacy self-management. *Big Data & Society, 2*(2), 1-16

*Pagallo, U. (2013). Robots in the cloud with privacy: A new threat to data protection? *Computer Law & Security Review, 29*(5), 501-508.

PARO (2019). PARO therapeutic robot. PARO website, 2 January 2019. Retrieved from http://www.parorobots.com/

Pham, M. T., Rajić, A., Greig, J. D., Sargeant, J. M., Papadopoulos, A., & McEwen, S. A. (2014). A scoping review of scoping reviews: Advancing the approach and enhancing the consistency. *Research Synthesis Methods, 5*(4), 371-385.

Pinch, T. J., & Bijker, W. E. (1984). The social construction of facts and artefacts: Or how the sociology of science and the sociology of technology might benefit each other. *Social Studies of Science, 14*(3), 399-441.

Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday, 15*(1).

Reeves, B. (2004). *The media equation: How people treat computers, television, and new media like real people and places*. Stanford, CA: CSLI Publications.

Richards, N. (2013). The dangers of surveillance. *Harvard Law Review, 126*(7), 1945-1952.

Rouvroy, A. (2008). Privacy, data protection, and the unprecedented challenges of ambient intelligence. *Studies in Ethics, Law, and Technology,* 2(1).

*Rueben, M., Grimm, C., Bernieri, F., & Smart, W. (2017). A taxonomy of privacy constructs for privacy-sensitive robotics. *CoRR, abs/1701.00841*.

Rueben, M., Aroyo, A., Lutz, C., Van Cleynenbreugel, P., Schmölz, J., … & Smart, W. (2018). Themes and research directions in privacy-sensitive robotics. In *ARSO 2018: Proceedings of the 2018 IEEE Workshop on Advanced Robotics and its Social Impacts*.

*Sadasivam, R., Luger, T., Coley, H., Taylor, B., Padir, T., ... & Houston, T. (2014). Robot-assisted home hazard assessment for fall prevention: A feasibility study. *Journal of Telemedicine and Telecare, 20*(1), 3-10.

*Sanfeliu, A., Llácer, M. R., Gramunt, M. D., Punsola, A., & Yoshimura, Y. (2010). Influence of the privacy issue in the deployment and design of networking robots in European urban areas. *Advanced Robotics*, 24(13), 1873-1899.

*Schafer, B., & Edwards, L. (2017). "I spy, with my little sensor": Fair data handling practices for robots between privacy, copyright, and security. *Connection Science*, 29(3), 200-2009.

Scheutz, M. (2012). The inherent dangers of unidirectional emotional bonds between humans and social robots. In P. Lin, K. Abney und G. A. Bekey (Eds.), *Robot Ethics: The Ethical and Social Implications of Robotics* (pp. 205-222). Cambridge: The MIT Press.

*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.

Sharkey, A. J. C. (2016) Should we welcome robot teachers? *Ethics and Information Technology, 18*(4), 283-297.

*Sharkey, A. J. C. & Sharkey, N. (2010) The crying shame of robot nannies. *Interaction Studies, 11*(2), 161-190.

*Sharkey, A. J. C. & Sharkey, N. (2012b). The eldercare factory. *Gerontology*, 58(3), 282-288.

Simitis, S. (1987). Reviewing privacy in an information society. *University of Pennsylvania Law Review, 135*(3), 707-746.

Smith, H. J., Dinev, T. & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989-1015.

Smithers, T. (1997). Autonomy in robots and other agents. *Brain and Cognition, 34*(1), 88-106.

SoftBank Robotics (2019a). Pepper. SoftBank Robotics website, 2 January 2019. Retrieved from https://www.softbankrobotics.com/emea/en/pepper

SoftBank Robotics (2019b). NAO. SoftBank Robotics website, 2 January 2019. Retrieved from https://www.softbankrobotics.com/emea/index.php/en/nao

Suchman, L. A. (2007). *Human-machine reconfigurations: Plans and situated actions*. Cambridge: Cambridge University Press.

*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 *AAAI-07 Workshop on Human Implications of Human–Robot Interaction*.

Turkle, S. (2013). Sociable robots. Talk at *2013 AAAs Meeting*, video. Retrieved from http://www.solvingforpattern.org/2013/02/17/sherry-turkle-aaas-talk-on-sociable-robotics/

Westin, A. F. (1968). Privacy and freedom. *Social Work, 13*(4), 114-115.

Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook: The Internet privacy paradox revisited. *Information, Communication & Society, 16*(4), 479-500.

*Zsiga, K., Edelmayer, G., Rumeau, P., Péter, O., Tóth, A. & Fazekas, G. (2013). Home care robot for socially supporting the elderly. *International Journal of Rehabilitation Research, 36*(4), 375-378.

Acknowledgements

We would like to thank two anonymous peer reviewers who provided very helpful feedback on the paper throughout the revision process. Our gratitude also goes to the editors of the special issue on mobile media beyond mobile phones, Jordan Frith and Didem Özkul, for their vision on the topic and for enabling a fruitful review process.

FIGURES

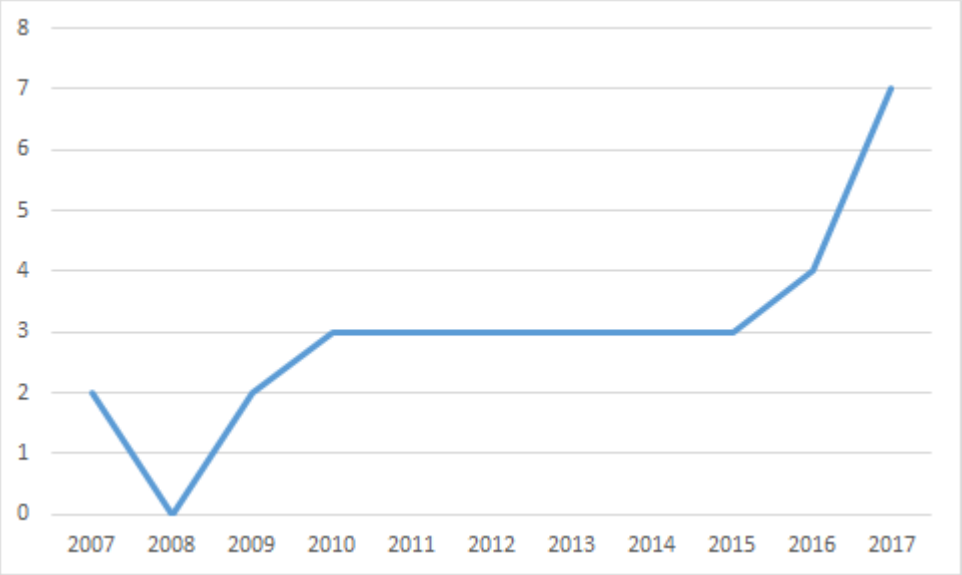

Figure 1: Number of publications per year

TABLES

Table 1: Overview of Interviewed Experts

Expert nr.	**Professional role**	**Gender**	**Country**	**Field**
1	PhD Student: public research university	Male	US	Robotics, engineering, HRI
2	Legal advisor: data protection agency	Male	Germany	Data protection law, consulting
3	Product expert: robotics company	Female	France	Industry, social robot development
4	Associate professor: public research university	Male	US	Law and technology, data protection
5	Professor: public research university	Male	UK	Ethics, philosophy, justice
6	Lecturer: public research university	Female	US	Law and technology, data protection

Table 2: Summary of Discipline, Analytical Approach and Robot Type

Items	**Frequency (Percentage)**
Discipline	Law - 10 (25.6) Computer science - 8 (20.5) Medicine and health sciences - 6 (15.4) Informatics/Information systems - 4 (10.3) Psychology - 4 (10.3) Political science - 3 (7.7) Robotics - 2 (5.1) Media and communication - 1 (2.6) Philosophy - 1 (2.6)
Analytical approach	Conceptual - 24 (72.7) Empirical - 9 (27.3)
Type of social robots investigated	Health robots - 10 (30.3), of which Elderly care - 7 (21.2) Social robots - 7 (21.2) Robots - 7 (21.2) Personal household robots - 4 (12.1) Robots for children - 2 (6.1) Educational robots - 1 (3) Unspecified - 2 (6.1)

Table 3: Summary and methodological preferences of the examined empirical studies (n=9)

Item	**Prevalence (% of total studies)**
Examined groups of people	Elderly people - 4 (33.3) Nursing staff - 3 (25) Potential end users - 1 (8.3) Adults - 1 (8.3) Parents - 1 (8.3) University staff - 1 (8.3) Not applicable - 1 (8.3)
Approach	Qualitative - 7 (77.8) Combined - 2 (22.2)
Main method applied	Focus groups - 2 (22.2) Survey - 2 (22.2) Combined - 2 (22.2) Interviews - 2 (22.2) Experiment - 1 (11.1)
Geographical place(s) of data collection	USA - 5 (55.6) Austria, France, Hungary - 1 (11.1) France, Netherlands, UK - 1 (11.1) UK, Greece, India, Pakistan, Indonesia - 1 (11.1) Not specified - 1 (11.1)
Sample size	Median: n= 41.25; n=9; 10; 12; 18; 18; 32; 108; 123; not applicable - 1
Type of robot examined	Nursing robots - 4 (44.4) Household robots - 4 (44.4) Toys - 1 (11.2)

Table 4: Overview of Privacy Implications in Literature Review and Expert Interviews

Type of Privacy	**Aspects Discussed**	**Example Studies**
Informational Privacy	amount of data; sensitivity of data; security risks: hacking; cloud connectivity; third-party access; intransparency: collecting unknown types of data; lack of user understanding	Pagallo, 2013; Syrdal et al., 2007
Psychological Privacy	psychological dependence; chilling effects; reduced self-reflection and human autonomy; particular concerns for vulnerable user groups such as children	Calo, 2011; Kaminski, 2015
Social Privacy	social bonding between robot and user; affection and trust can lead to the revelation of secrets	Lee et al., 2011; Sharkey, 2016
Physical Privacy	access to private rooms; capacity to access areas users themselves cannot access; uncomfortable closeness	Hoffmann, 2013; Sedenberg et al., 2016

APPENDIX

Interview Guideline

Introductory questions

1) What personal experiences have you already had with social robots?

2) What do you mean by the term "social robot"? What kinds and examples come to your mind?

3) How can social robots increase the user's quality of life?

4) In which areas can social robots help users?

5) What is your understanding of privacy?

6) How can social robots affect user privacy?

7) What is so different about social robots in this regard? How can this be compared with other
technologies such as smartphones for example?

8) What impact can social robots have on the perception or feelings of users?
a. Emotional relationship with social robots
b. Uncertainty, suspicion, no retreat in the home

9) How secure are currently available social robots in terms of hacking in your opinion?

Privacy and the user

10) How actively does the user actually protect their privacy in practice?

11) Can the protection of their privacy be left to the users themselves?

12) How are users adequately informed about interventions in their privacy?

13) How has the relevance of privacy changed with new technologies?

14) How can the user's privacy be protected through the programming of the social robot?

Data ownership

15) Who do you think should own the data collected by social robots?

16) How are users adequately informed who owns their data and what it is used for?

Legal framework

17) How is the privacy of users legally protected in home or office situations?

enquiry on demand, depending which areas the interviewees are active in

a. In Germany

b. At EU level

c. According to US jurisprudence

18) What are the implications of these legal frameworks for innovation?

a. Is the current legal situation hindering innovations?

b. Are there differences between different countries?

19) Is there a risk that the state can gain access to data collected by social robots?

Outlook

20) How can users' privacy be protected at the legal level in the future?

21) Which technical protection mechanisms, for example programming, do you consider to be useful and technically feasible in the future?

22) How can users be sensitized or educated and a change in their behavior can take place?

23) What steps do businesses need to take to protect the privacy of users of their products?

References in the systematic literature review not cited in the text

Armbrust, C., Mehdi, S. A., Reichardt, M., Koch, J. & Berns, K. (2011). Using an autonomous robot to maintain privacy in assistive environments. *Security and Communication Networks, 4*(11), 1275-1293.

Kahn, P. H., Ishiguro, H., Friedman, B. & Kanda, T. (2007). What is a human? – Toward psychological benchmarks in the field of human-robot interaction. *Interaction Studies*, 8(3), 363-390.

Kernaghan, K. (2014). The rights and wrongs of robotics: Ethics and robots in public organizations. *Canadian Public Administration*, 57(4), 485-506.

Körtner, T. (2016). Ethical challenges in the use of social service robots for elderly people. *Zeitschrift für Gerontologie und Geriatrie, 49*, 303-307.

Sharkey, A. J. C. & Sharkey, N. (2012a). Granny and the robots: Ethical issues in robot care for the Elderly. *Ethics and Information Technology, 14*(1), 27-40.

Sharkey, N. (2008). The ethical frontiers of robotics. *Science, 322*(5909), 1800-1801.

Sorell, T. & Draper, H. (2017). Second thoughts about privacy, security and deception. *Connection Science, 29*(3), 217-222.

References found through wildcard operators and Scopus search

Fernandes, F. E., Yang, G., Do, H. M. & Sheng, W. (2016). Detection of privacy-sensitive situations for social robots in smart homes. In *IEEE International Conference on Automation Science and Engineering* (pp. 727-732). New York: IEEE.

Koops, B.-J., Di Carlo, A., Nocco, L., Casamassima, V. & Stradella, E. (2013). Robotic technologies and fundamental rights: Robotics challenging the European constitutional framework. *International Journal of Technoethics, 4*(2), 15-35.

Leite, I., & Lehman, J. F. (2016). The robot who knew too much: Toward understanding the privacy/personalization trade-off in child-robot conversation. In *Proceedings of the 15th International Conference on Interaction Design and Children* (pp. 379-387). New York: ACM.

Van Nus, M. (2016). Social robots, privacy, and ownership of data: Some problems and suggestions. In J. Seibt, M. Nørskov, & S. Schack Andersen (Eds.), *What Social Robots Can and Should Do* (pp. 190-191). Amsterdam: IOS Press.