Felix Carros, Anne Wierling (2023): Social Robots in Care and Data Privacy – A European Perspective. 9th International Conference on Infrastructures in Healthcare, DOI: 10.48340/ihc2023_p009

Social Robots in Care and Data Privacy – A European Perspective

Felix Carros[1,2], Anne Wierling[1]
[1]University of Siegen, [2]Fraunhofer FIT
{felix.carros, anne.wierling}@uni-siegen.de

Abstract. Social Robots increasingly become a challenge for data privacy regulations within care facilities, as they are not prepared for robots that can scan their surroundings and possibly share this data in real-time. The needs of stakeholders to these emerging challenges must be analyzed to apply existing data privacy rules. We collected data from stakeholders through interviews (n=66), surveys (n=271), and workshops (n=39). The data was analyzed towards opinions of data privacy concerning robots in care facilities. Our findings have then been contrasted to existing data privacy regulations (GDPR) in Europe and show how the needs of the stakeholders towards such systems can be harmonized with the existing rules and what additional regulation is needed. This study enables a better understanding of the expectations and challenges of social robots regarding data privacy.

Introduction

With recent developments in social robotics, it is likely that such systems increasingly become prevalent in the care sector. Robots are seen as potentially supporting for caregivers or people in need of care (e.g., guiding physical and cognitive training, communicating information, companionship, and religion (see Coghlan et al. (2018); Helm et al. (2022); Trovato et al. (2021, 2018); Moharana et al. (2019); Carros et al. (2020, 2022a)). In all these applications, we argue, that ethical, legal, and social aspects must be considered in addition to questions of technical feasibility. A key challenge in this area is providing users with a solution that supports them and improves their well-being while at the same time ensuring data protection and privacy (Störzinger et al. (2020); Carros et al. (2022b)). This is important not only because the General Data Protection Regulation (GDPR) is a

legal requirement in Europe, but also because it is required to be acceptable in care environments. This paper explores the attitudes of stakeholders (caregivers, insurances, older adults, doctors, and other professions surrounding the care sector) about the usage of social robots in care about data protection and privacy. We discuss the potential challenges posed by GDPR and, for this purpose, we analyzed qualitative and quantitative data (e.g., survey results, interviews, and field observations) obtained during the course of our work. The aim is to compare the present GDPR legislation to the elements identified by stakeholders about data protection and privacy that are necessary for effective and accepted robot use.

Context

Our study is located at the intersection of three research areas: 1) The increasing use of robots in the context of care; 2) research on users' attitudes towards privacy issues; and 3) the current legal framework and practical challenges of data protection.

Numerous concepts, projects, prototypes, and established solutions already exist in the field of robotics in the care setting. However, they are, for the most part yet to be fully established in the routine practices of caregivers. The spectrum of applications is diverse and ranges from commercial robots for logistical support to robots talking and playing with care recipients. Robots can not only assist in functional tasks such as bathing (e.g., Satoh et al. (2009)) or dementia care (e.g., Felzmann et al. (2015)) but also become social interaction partners (e.g., Aminuddin et al. (2016); Carros et al. (2023)). However, to integrate these potential solutions fully a legal base is needed. Within Europe, the regulation of GDPR is working as a legal frame. We identified some functions of robots in care settings that will make this legal implementation difficult and propose alternatives in the discussion.

Widespread concern has been expressed about privacy issues and the use of personal data (e.g., Lanchester (2017); Zuboff (2019); Landwehr et al. (2019)). In addition to well-known issues surrounding Facebook and other social media, there is some evidence that factors such as loyalty programs, trust in marketers, and other benefits influence people's decisions to share their data (Chanhoo Song and Chan Ik Park (2006); Fathi et al. (2013)). It has been shown that people are more willing to disclose information such as names and demographic information than, for example, financial information (Phelps et al. (2000)). Such concerns are also manifest in the context of healthcare (Abouelmehdi et al. (2017); Hathaliya and Tanwar (2020)), largely because of the enormous potential value of user data. This can also be observed in the care sector, research has shown that many have reservations about giving out personal data (e.g., Pickard and Swan (2014); Shen et al. (2019); Müller et al. (2010)).

Since May 2018, the General Data Protection Regulation (GDPR) has protected the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data in the European Union. Processing the personal data of robots in care contexts falls within the scope of the GDPR. Since robots in care contexts often require monitoring systems, particular attention must be paid to data protection and data security (Ethikrat (2020); BMFSFJ (2020)). From a legal

perspective in Europe, the robot manufacturer as well as care institutions and operators are considered responsible parties and thus addressees of data protection obligations (Steinrötter (2020)). One example of such an obligation is voluntary and informed consent, which is central to the legal conformity and processing of personal data. Several challenges arise here in practice. For example, an "information overload" must be counteracted (Steinrötter (2020)). In addition to the question of whether informed consent is still possible at all or whether "information overload" can be reduced, lawyers have also questioned the balance between the personal rights of individuals and the potential benefits of big data—as well as the question of the extent to which individuals can make sovereign decisions about the use of their data (Marckmann (2020)).

Our study contributes to the ongoing research by uniting these topics and focusing on data protection and privacy for the use of robots in care contexts. We contrast the results from our empirical work with stakeholders of the care sector to the existing GDPR regulations and develop additions to the existing legislation to give suggestions on how the regulation should accommodate the use of care robots within this sensitive field.

Methods

The results presented in this paper are based on three types of data (interviews, statements in workshops, and a quantitative questionnaire). A mixed method approach was chosen (Schensul and LeCompte (2013)) to combine the data. The qualitative data in particular add insight and show the concrete opinions of the participants on topics regarding data protection in care robots. The quantitative data support these statements and show that the statements are supported by a larger group. None of the data sets are considered representative. The participants were thematically related and did not correspond to the cross-sections of society.

Data sources

The data shown in this paper were based on four different data sources: 1. Interviews 2. Questionnaire 3. Questions during workshop 4. Follow-up Survey. The interviews (Data source 1) were conducted with 66 stakeholders from the care sector. They were carried out in 2018, based on a project which was concerned with science communication. For this purpose, the robot Pepper (humanoid robot) and its care programs were presented to a broad public. This included the demonstration of the robot at fairs and events with the themes of care and IT. At these events, interested visitors were asked for an interview. Since the events were thematically focused on care, most interviewees were employed in this sector or otherwise had some connection to it. Interviews typically lasted for 20-30 minutes. The questionnaire (Data source 2) with 250 persons was administered at the same events but who preferred to fill out a questionnaire.

Then we asked questions about privacy and related matters during workshops (Data source 3), all concerned with care robotics. The participants (39) came from two different backgrounds, comprising both older adults and upper-school students.

The participants were not employed in the sector, but they did have prior knowledge of the topic through personal experience. Lastly, we did a follow-up survey (Data source 4) with the same participants and received 21 responses.

During interviews and workshops, all participants were confronted with social robots and their potential application. They were able to experience the robots in action or touch them and could ask researchers questions about them and their field of application.

Procedure of Data Analysis

All interviews were transcribed and analyzed using reflexive thematic analysis (Braun et al. (2018)). The transcripts were processed with MaxQDA and the categories were established deductively. The quantitative evaluation was carried out with the help of Excel. All statements that the participants made were categorized according to four major thematic fields: (1) Ideas and conceptions about the functions or the purposes of the robot; (2) Weighing the benefits of the robot against the privacy of the person concerned; (3) Informed consent; (4) Attribution of responsibility.

Results

Robot as Monitoring Tool

The first function of the robot mentioned by some interviewees was the monitoring of the residents in the care home. For example, P48 (Management, Care Company) saw the robot as a monitoring technology for the care workers: *"I can also imagine that they are on the move in living areas and that I, as a nurse, can look over the face or the camera when I am providing care in a room: are the residents still sitting in their chairs or has someone slipped down or something?"*. She was not alone with this opinion, P54 (Management, Care Company) classified the use of robots in nursing similarly: *"To cover safety topics, i.e., as a safety guard who makes rounds and checks whether everything is in order[...]"*. But, while this seems like a convenient use case, P18 (Family Member of Person in need of care) saw it differently and thought that the robot is: *"[...] Like a surveillance camera in the room, just different."*.

P46 (Quality Management, Care Company) could even imagine robots seeking help for the residents and reacting to voices or vibrations: *"[...] at least now there is this robot that fetches help. I mean, there are already these alarm buttons that call for help and things like that, but you just know that there is someone who has a sensor system that responds to a voice or really notices when someone falls or things like that."*

The ability to decide for oneself how much and to what extent a robot collects and stores data was important to the participants; P48 (Management, Care Company) mentioned that *"You also have to have the possibility to be unobserved."* In line with this statement, P49 (Accountant, Care Company) discussed the importance of default settings to ensure data protection, elaborating that *"[...] I*

would like to determine for myself in which time window and I would also like to determine for myself from when to when [...] It could also be that I am at risk of falling and say that I don't want to use the motion detector, thus accepting that I might fall and that I might not be found until a little later. So, I would like to have these possibilities."

Trade-off between Benefit and Privacy

Several interviewees described data protection as an ambiguous issue that, on the one hand, is critical for protecting older adults' rights and data. However, it is difficult to put into practice. For instance, P15 (Employee, NGO in Care Sector) stated that *"How to cope with data storage is always an ambiguous problem. I believe you must weigh the benefits it brings."* Similar points were made by P24 (Employee, IT Company in Care Sector): *"I think we should be careful about security and data protection on the one hand. On the other hand, we should not let this stop us from actually doing something good for people."* P26 (Student of IT) agreed with these comments, adding that *"[...] it's a balancing act between wanting to offer people more services or saying, okay, there are a lot of possibilities where we could help you, but for that, we also need this information."*

The respondents thus weighed the benefits of the robot against the intrusion of privacy that they would represent for the person using it. In this consideration, it is important to note that the privacy of care home residents is already affected — whether by different caregivers, social service workers, or doctors, who tend to come into the rooms of the residents on very short notice without waiting for an answer when they knock on the door. In some cases, it may be less unpleasant for a person to ask a robot for assistance than to ask someone working in a care home. Accordingly, P16 (Neuroscientist) saw a great benefit in a robot's freedom of evaluation: *"I could even say that acceptance is even greater because of shame. So, let's say you feel yourself to be unaesthetic and ashamed. But if a robot is there, you might have less shame."*

The willingness to make data available (acceptance of data processing) is greater if the people concerned expect a great benefit. For instance, P54 (Management, Care Company) explains that the benefits of the robot can outweigh the disadvantages, especially in emergencies: *"[...] especially when it came to the health card in particular, there was a great willingness to store things, be it an X-ray or a medication plan, blood group, etc., so that information can be exchanged as quickly as possible. Especially when there are emergencies."*

At the workshop, almost all respondents thought that the purpose of health monitoring would justify the use of a robot, or that the purpose to be fulfilled was rated as more important than the invasion of privacy.

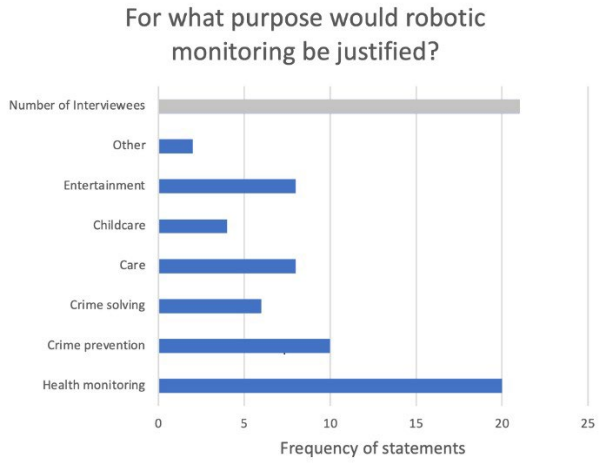

Figure 1: Justifications for monitoring. n=21.

Non-functional Acceptance Criteria

The interviewees saw additional requirements that needed to be fulfilled for social robots to be acceptable. They referred to data security, to the transfer of data, to the storage of data as well as to "privacy by design" aspects. These requirements do not fulfill a function in the sense of a purpose; rather, they represent prerequisites that, in the opinion of the respondents, ensure the robot can be used at all. P16 (Neuroscientist), for instance, felt that data security or the location of personal data storage plays an important role in connection with the use of robots: *"The moment a robot is connected to the network, the question is, all the things you entrust to the robot, how confidential is that? And does a clinic have any security at all [...] not that it is stored on Google, Facebook, and the like."*

Regarding data collection P47 (Management, Care Company) discussed the concept of privacy by design, explaining that *"You have to be able to say exactly up to here the robot is allowed to record, up to here the robot is allowed to search. In which cloud is it saved, the video, is it saved at all, that must be precisely documented and also adjustable. So that I can say myself, up to here and no further."* P49 (Accountant, Care Company) agreed with this statement: *"[...] As long as I can say, I don't want the robot now and it goes out and maybe it has a big button somewhere that you can also see [to switch off]".*

These statements show that robotic systems in care environments need to be transparent about the data they collect and the way they are stored, analyzed, and transmitted.

Discussion

The results showed that stakeholders view the robot as a useful tool for monitoring people in need of care or for making rounds at care homes to perform check-ups or answer questions. Further, the robot was seen as useful to assist residents and to call for help in case of an emergency. However, the interviewed also foresaw restrictions on the usage of robots, believing that there must be transparency regarding where

any recorded data are being sent and that there must be an option to stop the recording of data at any time. This raises important questions about what data is to be recorded, how it is stored, and, above all, who has access to it. Nursing, after all -and whether it is institutional- involves several practitioners with varying degrees of medical knowledge and different kinds of organizational affiliation. Data may also, in some instances, be shared with 3rd parties such as kit suppliers or external medical facilities.

With the GDPR, data protection has been harmonized and adapted across Europe. This was intended to generate "solutions to questions raised by 'Big Data' and new techniques or types of data processing such as profiling, web tracking or cloud computing for the protection of privacy" (BMWI (2021)). The focus of this regulation is the "fundamental right to informational self-determination through greater transparency and more co-determination of citizens with regard to their data" (BMWI (2021)). Through this, an important step has been taken to better protect the fundamental rights of those affected. Since nearly every use of social robots in a care context requires the processing of personal data, the GDPR also applies in these cases. In the following sections, we discuss the results and contrast them to the current state of the law of GDPR. By doing so we show where the current regulations make the use of robotic systems difficult and derive some possible solutions to it.

Self-Determination - Trade-off between benefit and privacy

The usage of a robot in the care context was seen as a trade-off where less privacy is traded for a higher quality of care. Until now, care always involves some reduction of privacy since, even without technology, care workers are necessary and, by definition, their presence involves some intrusion on privacy. However, the problem with the use of robots is that, theoretically, the private information they are privy to could be easily shared with people with malicious intent. It is evidently the case that access rights will need to be managed in some way. Nevertheless, participants also discussed privacy advantages, including that some people might feel less shame being helped (e.g., going to the bathroom).

For care home residents it is often not transparent what data are collected and stored by social robots and for what function it is used. This applies not only to the use of robot technologies but currently to vast parts of the internet as well (Fiesler and Hallinan (2018)). Data protection itself is a sensitive, complex, and, above all, ambivalent issue in the use of social robots in the care sector. On the one hand, it is essential to protect and respect the rights of people in need of care. On the other hand, effective assistance for caregivers (and residents) through robot technologies (and tailored to individual needs and concrete situations) typically requires the processing of data. This data must usually be made accessible to a larger group of people, and their usefulness and potential misuse must be constantly monitored. As the results showed, the stakeholders in this field are aware of this trade-off and rely on legislation to ensure that it is not to their disadvantage.

Self-determination was significant for the stakeholders interviewed; self-determined action requires a certain degree of understanding. This is due to the fact that data processing is often non-transparent, and the user can be unaware or only

superficially aware of it. In this respect, a pronounced digital competence is necessary for self-determination. Such competence is not strongly developed within the group of people in need of care. Although studies have shown that adaptation to new technology by this group has occurred faster than was previously assumed, the group nevertheless has a lower affinity for technology than the average in society Golant (2017). There are many reasons for this. One is that some may lack understanding about modern media technology Kim et al. (2016); Pang et al. (2021). That said, other factors also play a role, such as how and with whom they use the technology (e.g., Schwaninger et al. (2022)). In this respect, transparency of data processing is particularly important for this group. Technology providers, we argue, must ensure that their solution is transparent so that this group can- as far as possible- make an informed, self-determined decision.

However, the controller of the robot could also base data processing on permission other than consent. In such a case, the data subject would no longer be able to decide for himself whether the personal data should be processed. It is conceivable within the framework of legal bases for lawful processing, for example, for the legitimate interests, the fulfillment of a contract, or the protection of vital interests of the data subject to be used instead. It is questionable whether the processing is necessary in the first two cases and whether consent is not obtainable in the case of the protection of vital interests (according to Recital 46 GDPR).

In case a robot can process personal data offline more efficiently than, for example, one or more humans could, it can be discussed whether the use of the robot is desirable under the GDPR. It may be that the robot requires much less data to achieve the same result as a human. Or it may, conversely, require just as much data as a human, but can collect it much faster. Since one of the principles of the GDPR is data minimization (Art. 5 I lit. c GDPR), it could be argued that this principle indirectly dictates or requires the use of new technology (Meents (2020)).

Classification of Data

If the assumption that robots need less data than caregivers is true, this could lead to a more frequent use of legitimate interests (Art. 6 I lit. f GDPR) as an element of permission for the use of a digital care assistant by the data controller. This, in turn, would harm the self-determination wishes of the persons concerned.

If it is a matter of processing sensitive data, the choice of permissions is more limited for the controller (Art. 9 II GDPR) than if he/she/it wants to process general personal data, as Art. 6 of the GDPR no longer applies. An essential difference in Art. 6 of the GDPR is that it provides no possibility to base processing on legitimate interests or contract performance.

Since sensitive data are usually involved in the area of social robots in care (e.g., the body mass index can quickly be calculated from general data such as weight and height), the explicit consent of the data subject (Art. 9 II lit. a GDPR) should be considered an element of permission. There are other possible legal bases for lawful processing under Art. 9 of the GDPR, for example, the protection of vital interests (Art. 9 II lit. c GDPR). If the controller can also base the data processing on legal permission of Art. 9 II GDPR, the consent of the data subject is no longer necessary (or, in relation to Art. 9 II lit. c GDPR, the protection of vital interests may not even

be possible), which would in turn run counter to the data subject's wishes for self-determination.

Here, an individualization of the classification of data, which is in the existing law not envisaged, could be conceivable. For one person, bank data are essentially in need of protection, while for another, data on lifestyle habits would be more important. Nevertheless, they are both considered general data and are not classified as sensitive data under the GDPR. It is conceivable that data subjects would be able to weigh the data being collected prior to processing regardless of whether the GDPR classifies the data as sensitive. For example, the controller could list all categories of data, and the data subject would mark the categories of data that he/she/it considers particularly worthy of protection. All unmarked data would be treated as general data, and all marked data would be treated as sensitive data (Loh (2020)). This individualization could influence the resulting possible permissions: all processing that relates to marked data requiring special protection that then requires authorization under Article 9 of the GDPR. If, however, the processing relates to general or unmarked data, a permissive element from Art. 6 of the GDPR is sufficient.

In this way, the person in need of care could increase their chance of making self-determined decisions by classifying general data as sensitive. This would influence the choice of permissions for the controller and increase the chance of (explicit) consent. This, in turn, would be at the expense of the information content since such a "data category upgrade" should only be possible if the data subject has a corresponding understanding of the facts and all the consequences involved in the decision (the same applies to "data category downgrade").

Conclusion

In the above, we have rehearsed the attitudes, beliefs, and preferences expressed by several stakeholders concerning data protection. Although the context we have discussed is a specific one, where GDPR regulation governs decision-making, the complexities we have discussed have much wider ramifications.

Transparent handling of the functions of social robots is essential in the event that these technologies are used. In our case, the federal government, as well as the Council of the European Union and the European Parliament in addition to the subsequent data controllers who must comply with the provisions of GDPR, bear great responsibility for defining the concrete framework conditions for using these technologies. In any case, a significant number of issues need to be resolved if robotic care is ever to be widespread, as other researchers also have recognized (e.g., Papadopoulos et al. (2020); Schwaninger (2020); Marchetti et al. (2022); Maibaum et al. (2022)). A wide range of professional, institutional, family, and personal interests need to be managed so that clear lines of right and responsibility can be drawn. These interests start with manufacturers and distributors, extend through institutional responsibilities, through to medical interventions and the attendant roles, down to routine caregiving and the rights of individuals and their families. Policy decisions in terms of how these complex rights and responsibilities are to be managed are, yet not fully understood and yet will have important

consequences for the emerging robotic technology. What matters need to be made clear to the individual user and, above all, to the people in need of care, how what data are collected and stored as well as when, how, and for what purpose, are all yet to be managed.

Furthermore, the older people who come into contact with the robot must be informed in simple language of what data are processed in this context and what they are used for. They should be given the choice of whether to consent and if they would classify the processed personal data as general or sensitive. At the same time, they should be given the option of deciding for themselves when and under what conditions a more data-saving variant of data processing should be used. Furthermore, both the controller and the manufacturers of the robots should be held responsible for complying with the privacy by design requirements of the GDPR.

Acknowledgments

We are grateful to everyone involved in this work. The knowledge of this publication was created in a collaborative effort. We are thankful for the given opportunity.

The presented work has partly received funding from the BMWK under grant agreement no. 01MF22009A.

References

Abouelmehdi, K., A. Beni-Hssane, H. Khaloufi, and M. Saadi (2017): ‘Big data security and privacy in healthcare: A Review’. *Procedia Computer Science*, vol. 113, pp. 73–80.

Aminuddin, R., A. Sharkey, and L. Levita (2016): ‘Interaction With the Paro Robot May Reduce Psychophysiological Stress Responses’. In: *The Eleventh ACM/IEEE International Conference on Human Robot Interaction*. p. 593–594, IEEE Press.

BMFSFJ (2020): ‘Achter Altersbericht: Ältere Menschen und Digitalisierung’.

BMWI (2020, last access: 12.03.2021): ‘Europäische Datenschutz-Grundverordnung’.

Board, E. D. P. (2020): ‘Guidelines 05/2020 on consent under Regulation 2016/679’.

Braun, V., V. Clarke, N. Hayfield, and G. Terry (2018): *Thematic Analysis*, pp. 1–18. Singapore: Springer Singapore.

Carros, F., B. Bürvenich, R. Browne, Y. Matsumoto, G. Trovato, M. Manavi, K. Homma, T. Ogawa, R. Wieching, and V. Wulf (2023): ‘Not that Uncanny After All? An Ethnographic Study on Android Robots Perception of Older Adults in Germany and Japan’. In: *Social Robotics: 14th International Conference, ICSR 2022, Florence, Italy, December 13–16, 2022, Proceedings, Part II*. pp. 574–586.

Carros, F., J. Meurer, D. Löffler, D. Unbehaun, S. Matthies, I. Koch, R. Wieching, D. Randall, M. Hassenzahl, and V. Wulf (2020): ‘Exploring Human-Robot Interaction with the Elderly: Results from a Ten-Week Case Study in a Care Home’. In: *Proceedings of the 2020 CHI Conference on*

Human Factors in Computing Systems. New York, NY, USA, p. 1–12, Association for Computing Machinery.

Carros, F., I. Schwaninger, A. Preussner, D. Randall, R. Wieching, G. Fitzpatrick, and V. Wulf (2022a): 'Care Workers Making Use of Robots: Results of a Three-Month Study on HumanRobot Interaction within a Care Home'. In: *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. New York, NY, USA, Association for Computing Machinery.

Carros, F., T. Störzinger, A. Wierling, A. Preussner, and P. Tolmie (2022b): 'Ethical, Legal & Participatory Concerns in the Development of Human-Robot Interaction'. *i-com*, vol. 21, no. 2, pp. 299–309.

Chanhoo Song, C. N. and E. L. Chan Ik Park (2006): '"Consumers' Privacy Concerns and Willingness to Provide Marketing-Related Personal Information Online"'. In: *NA - Advances in Consumer Research Volume 33, eds. Connie Pechmann and Linda Price, Duluth, MN*. pp. Pages: 212–217, Association for Consumer Research.

Coghlan, S., J. Waycott, B. B. Neves, and F. Vetere (2018): 'Using Robot Pets Instead of Companion Animals for Older People: A Case of 'Reinventing the Wheel'?'. In: *Proceedings of the 30th Australian Conference on Computer-Human Interaction*. New York, NY, USA, p. 172–183, Association for Computing Machinery.

Cohen, S. (2013): 'Nudging and Informed Consent'. *The American Journal of Bioethics*, vol. 13, no. 6, pp. 3–11.

Douglas, C. and E. Proudfoot (2013): 'Nudging and the Complicated Real Life of "Informed Consent"'. *The American Journal of Bioethics*, vol. 13, no. 6, pp. 16–17.

Dworkin, G. (2020): 'Paternalism'. In: E. N. Zalta (ed.): *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, Fall 2020 edition.

Erica Palmerini, Federico Azzarri, F. B. A. B. A. C. J. C. F. C. A. D. C. M. C. M. C. B.-J. K. F. L. N. M. L. N. A. P. H. S. P. S. M. S. and K. Warwick (2012): 'Deliverable 6.2 of the project RoboLaw'.

Ethikrat, D. (2020): 'Stellungnahme Robotik für gute Pflege', pp. 18.

Eyal, N. (2019a): 'Informed Consent'. In: E. N. Zalta (ed.): *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, Spring 2019 edition.

Eyal, N. (2019b): 'Informed Consent In E. N. Zalta (Hrsg.)'.

Fathi, S., A. Sanayei, and M. Siyavooshi (2013): 'SMS Advertising and Consumer Privacy: Analysis of Factors Affecting Consumer Willingness to send and Receive Information in Permission and Data based SMS advertising'. *New Marketing Research Journal*, vol. 3, pp. 101–124.

Felzmann, H., K. Murphy, D. Casey, and O. Beyan (2015): 'Robot-assisted care for elderly with dementia: is there a potential for genuine end-user empowerment?'.

Fiesler, C. and B. Hallinan (2018): *"We Are the Product": Public Reactions to Online Data Sharing and Privacy Controversies in the Media*, p. 1–13. New York, NY, USA: Association for Computing Machinery.

Gerling, K., D. Hebesberger, C. Dondrup, T. Kärtner, and M. Hanheide (2016): 'Robot deployment in long-term care'. *Zeitschrift für Gerontologie und Geriatrie*, vol. 49, no. 4, pp. 288–297.

Golant, S. M. (2017): 'A theoretical model to explain the smart technology adoption behaviors of elder consumers (Elderadopt)'. *Journal of Aging Studies*, vol. 42, pp. 56–73.

Haag, Ina & Hauser, A. (2019): *Datenschutz im Krankenhaus- mit allen Neuerungen durch die DSGVO*. Düsseldorf: Deutsche Krankenhaus Verlagsgesellschaft mbH.

Hathaliya, J. J. and S. Tanwar (2020): 'An exhaustive survey on security and privacy issues in Healthcare 4.0'. *Comput. Commun.*, vol. 153, pp. 311–335.

Helm, M., F. Carros, J. Schädler, and V. Wulf (2022): 'Zoomorphic Robots and People with Disabilities'. In: *Proceedings of Mensch Und Computer 2022*. New York, NY, USA, p. 431–436, Association for Computing Machinery.

Kachouie, R., S. Sedighadeli, R. Khosla, and M.-T. Chu (2014): 'Socially Assistive Robots in Elderly Care: A Mixed-Method Systematic Literature Review'. *International Journal of HumanComputer Interaction*, vol. 30, no. 5, pp. 369–393.

Kanamori, M., M. Suzuki, and M. Tanaka (2002): 'Maintenance and Improvement of Quality of Life among Elderly Patients Using a Pet-Type Robot.'. *Nippon Ronen Igakkai Zasshi. Japanese Journal of Geriatrics*, vol. 39, no. 2, pp. 214–218.

Kapsner, A. and B. Sandfuchs (2015): 'Nudging as a Threat to Privacy'. *Review of Philosophy and Psychology*, vol. 6, no. 3, pp. 455–468.

Kaulartz, M. and T. Braegelmann (2020): *Rechtshandbuch Artificial Intelligence und Machine Learning* -. München: Beck C. H.

Kidd, C., W. Taggart, and S. Turkle (2006): 'A sociable robot to encourage social interaction among the elderly'. In: *Proceedings 2006 IEEE International Conference on Robotics and Automation, ICRA*. IEEE.

Kim, S., K. Z. Gajos, M. Muller, and B. J. Grosz (2016): 'Acceptance of Mobile Technology by Older Adults: A Preliminary Study'. In: *Proceedings of the 18th International Conference on Human-Computer Interaction with Mobile Devices and Services*. New York, NY, USA, p. 147–157, Association for Computing Machinery.

Lanchester, J. (2017): 'You are the product. London Review of Books 39, no. 16'.

Landwehr, M., A. Borning, and V. Wulf (2019): 'The High Cost of Free Services: Problems with Surveillance Capitalism and Possible Alternatives for IT Infrastructure'. In: *Proceedings of the Fifth Workshop on Computing within Limits*. New York, NY, USA, Association for Computing Machinery.

Lin, J., W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao (2017): 'A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications'. *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142.

Loh, W. (2020): 'Informed Consent and robotics in Elder Care'. In: *Tnternationale Klausurwoche: „Neue ethische Herausforderungen in der datenreichen Forschungsmedizin: ein Ländervergleich"*. BMBF Klausurwoche.

Maibaum, A., A. Bischof, J. Hergesell, and B. Lipp (2022): 'A critique of robotics in health care'. *AI & society*, pp. 1–11.

Marchetti, E., S. Grimme, E. Hornecker, A. Kollakidou, and P. Graf (2022): 'Pet-Robot or Appliance? Care Home Residents with Dementia Respond to a Zoomorphic Floor Washing Robot'. In: *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. New York, NY, USA, Association for Computing Machinery.

Marckmann, G. (2020): 'Ethische Fragen von Digital Public Health'. *Bundesgesundheitsblatt Gesundheitsforschung - Gesundheitsschutz*, vol. 63, no. 2, pp. 199–205.

Matteo, D. D., A. Fine, K. Fotinos, J. Rose, and M. Katzman (2018): 'Patient Willingness to Consent to Mobile Phone Data Collection for Mental Health Apps: Structured Questionnaire'. *JMIR Mental Health*, vol. 5, no. 3, pp. e56.

Meents, J. G. (2020): 'Datenschutz durch KI'. In: Kaulratz and Braegelmann (eds.): *Rechtshandbuch Artificial Intelligence und Machine Leanrning*. München: Beck C. H., p. 451.

Moharana, S., A. E. Panduro, H. R. Lee, and L. D. Riek (2019): 'Robots for Joy, Robots for Sorrow: Community Based Robot Design for Dementia Caregivers'. In: *2019 14th ACM/IEEE International Conference on Human-Robot Interaction (HRI)*. pp. 458–467.

Munoz, R., M. Fox, M. Gomez, and S. Gelfand (2015): 'Evidence-Based Nudging: Best Practices in Informed Consent'. *The American Journal of Bioethics*, vol. 15, no. 10, pp. 43–45.

Müller, C., L. Wan, and D. Hrg (2010): 'Dealing with wandering'. In: *Proceedings of the 16th ACM international conference on Supporting group work - GROUP '10*. ACM Press.

Pang, C., Z. Collin Wang, J. McGrenere, R. Leung, J. Dai, and K. Moffatt (2021): 'Technology Adoption and Learning Preferences for Older Adults: Evolving Perceptions, Ongoing Challenges, and Emerging Design Opportunities'.

Papadopoulos, I., C. Koulouglioti, R. Lazzarino, and S. Ali (2020): 'Enablers and barriers to the implementation of socially assistive humanoid robots in health and social care: a systematic review'. *BMJ open*, vol. 10, no. 1, pp. e033096.

Phelps, J., G. Nowak, and E. Ferrell (2000): 'Privacy Concerns and Consumer Willingness to Provide Personal Information'. *Journal of Public Policy & Marketing*, vol. 19, no. 1, pp. 27–41.

Pickard, K. and M. Swan (2014): 'Big Desire to Share Big Health Data: A Shift in Consumer Attitudes toward Personal Health Information'.

Pinto, P., R. Lages, and M. Au-Yong-Oliveira (2020): 'Web Cookies: Is There a Trade-off Between Website Efficiency and User Privacy?'. In: *Trends and Innovations in Information Systems and Technologies*. Springer International Publishing, pp. 713–722.

Pu, L., W. Moyle, C. Jones, and M. Todorovic (2018): 'The Effectiveness of Social Robots for Older Adults: A Systematic Review and Meta-Analysis of Randomized Controlled Studies'. *The Gerontologist*, vol. 59, no. 1, pp. e37–e51.

Radic, M. and A. Vosen (2020): 'Ethische, rechtliche und soziale Anforderungen an Assistenzroboter in der Pflege'. *Zeitschrift fürr Gerontologie und Geriatrie*, vol. 53, no. 7, pp. 630–636.

Sabanovic, S., C. C. Bennett, W.-L. Chang, and L. Huber (2013): 'PARO robot affects diverse interaction modalities in group sensory therapy for older adults with dementia'. In: *2013 IEEE 13th International Conference on Rehabilitation Robotics (ICORR)*. IEEE.

Satoh, H., T. Kawabata, and Y. Sankai (2009): 'Bathing Care Assistance with Robot Suit HAL'. In: *Proceedings of the 2009 International Conference on Robotics and Biomimetics*. p. 498–503, IEEE Press.

Schensul, J. J. and M. D. LeCompte (2013): *Essential Ethnographic Methods - A Mixed Methods Approach*. Lanham: Rowman Altamira.

Schwaninger, I. (2020): 'Robots in Older People's Living Spaces: Designing for Trust in Situated Human-Robot Interaction'. In: *Companion of the 2020 ACM/IEEE International Conference on Human-Robot Interaction*. New York, NY, USA, p. 600–602, Association for Computing Machinery.

Schwaninger, I., F. Carros, A. Weiss, V. Wulf, and G. Fitzpatrick (2022): 'Video connecting families and social robots: from ideas to practices putting technology to work'. *Universal Access in the Information Society*, pp. 1–13.

Shen, N., T. Bernier, L. Sequeira, J. Strauss, M. P. Silver, A. Carter-Langford, and D. Wiljer (2019): 'Understanding the patient privacy perspective on health information exchange: A systematic review'. *International Journal of Medical Informatics*, vol. 125, pp. 1–12.

Simkulet, W. (2018): 'Informed consent and nudging'. *Bioethics*, vol. 33, no. 1, pp. 169–184.

Steinrötter, B. (2020): 'Datenschutzrechtliche Implikationen beim Einsatz von Pflegerobotern. S. 337'.

Störzinger, T., F. Carros, A. Wierling, C. Misselhorn, and R. Wieching (2020): 'Categorizing Social Robots with Respect to Dimensions Relevant to Ethical, Social and Legal Implications'. *i-com*, vol. 19, no. 1, pp. 47–57.

Söbbing, T. (2019): *Fundamentale Rechtsfragen zur künstlichen Intelligenz - (AI Law)*. Fachmedien Recht und Wirtschaft, dfv Mediengruppe.

Trovato, G., L. De Saint Chamas, M. Nishimura, R. Paredes, C. Lucho, A. Huerta-Mercado, and F. Cuellar (2021): 'Religion and robots: Towards the synthesis of two extremes'. *International Journal of Social Robotics*, vol. 13, pp. 539–556.

Trovato, G., C. Lucho, A. Ramón, R. Ramirez, L. Rodriguez, and F. Cuellar (2018): 'The creation of SanTO: a robot with "divine" features'. In: *2018 15th International Conference on Ubiquitous Robots (UR)*. pp. 437–442.

Weber, R. H. (2010): 'Internet of Things – New security and privacy challenges'. *Computer Law & Security Review*, vol. 26, no. 1, pp. 23–30.

Yang, Y., L. Wu, G. Yin, L. Li, and H. Zhao (2017): 'A Survey on Security and Privacy Issues in Internet-of-Things'. *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258.

Zuboff, S. (2019): *The age of surveillance capitalism: The fight for a human future at the new frontier of power: Barack Obama's books of 2019.* Profile books.