INSTITUTE OF
MANAGEMENT
SCIENCE

Consideration of the Impact of Care Robots on Privacy

A Review of Current Literature

DIPLOMA THESIS

submitted in partial fulfillment of the requirements for the degree of

Diplom-Ingenieur

in

Mechanical Engineering - Management

by

Ing. Reinhard Grabler, BSc.
Registration Number 01028676

to the Faculty of Mechanical and Industrial Engineering

at the TU Wien

Advisor: Univ.-Prof. Mag. Dr. Sabine T. Köszegi

Vienna, 10th January, 2022

Reinhard Grabler

Sabine T. Köszegi

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Declaration of Authorship

Ing. Reinhard Grabler, BSc.

I hereby declare that I have written this Diploma Thesis independently, that I have completely specified the utilized sources and resources and that I have definitely marked all parts of the work - including tables, maps and figures - which belong to other works or to the internet, literally or extracted, by referencing the source as borrowed.

Vienna, 10th January, 2022

Reinhard Grabler

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU WIEN Bibliothek Your knowledge hub

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Acknowledgements

Thanks to my family and friends who had my back and kept me going while writing this thesis.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU WIEN Bibliothek Your knowledge hub

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Kurzfassung

Es steht ein demografischer Wandel bevor: Die Anzahl und auch der Anteil der älteren Menschen nimmt zu, was zu einem Mangel an verfügbaren informellen Pflegekräften führt. In der Forschung wurden vielversprechende Lösungen wie etwa Pflegeroboter, untersucht, die es ermöglichen Autonomie zu bewahren um zuhause zu altern. Zwar bringen Robotertechnologien viele Vorteile, jedoch könnten sie auch Privatsphäreverletzungen verstärken. Es ist Ziel dieser Arbeit einen Einblick darüber zu gewähren, wie in der aktuellen Literatur die Aspekte der Privatsphäre im Zusammenhang mit Pflegerobotern verhandelt werden. Publikationen aus den Jahren 2010 bis 2021 werden mittels qualitativer Kodierung analysiert, um die vorherrschenden Narrative, sowie auch die Abhilfestrategien zur Vermeidung von Privatsphäreverletzungen, zu analysieren.

In einer systematischen Literaturrecherche wurden die relevanten Beiträge zu den Themen Pflegeroboter, sozial assistierende Roboter und Ambient Assisted Living (AAL) Technologien ermittelt. Es wurden Metadaten entnommen und einen Überblick des Literaturbestands zu schaffen. Publikationen, welche wesentliche Beiträge zur Forschungsfrage lieferten, wurden im Volltext ausgewertet und die Inhalte detailliert diskutiert. Es zeigt sich dass ein großer Teil der Veröffentlichungen sich nur am Rande mit Privatsphäre befassen. Bedenken zu Überwachung und dem Aufstieg von künstlicher Intelligenz (KI) in Verbindung mit Big Data und maschinellem Lernen werden dringlich hervorgehoben. Letzteres könnte zu noch nie dagewesenen Herausforderungen für den Privatsphäreschutz führen.

Es wird eine Fülle von Abhilfestrategien erörtert: Transparenz, informierte Einwilligung, der Ansatz Privacy by Design (PbD) und kontextbezogene Integrität sind die am weitesten verbreiteten. Die praktische Anwendung dieser Strategien ist jedoch in der Regel ungeklärt und erfordert weitere Forschung. Privatsphäre wird meist entlang der informationellen und physischen Dimensionen verhandelt, während die soziale und psychologische Privatsphäre nicht ausreichend berücksichtigt werden. Dieses Ungleichgewicht spiegelt sich sowohl in der Diskussion über die vorhandenen Bedenken, als auch in den vorgeschlagenen Abhilfestrategien wider.

Im Allgemeinen besteht ein Konsens darüber, dass die Vorteile der Roboterpflegetechnologien das Risiko der Privatsphäreverletzung überwiegen. Es wird empfohlen mit Vorsicht vorzugehen und proaktiv statt reaktiv zu handeln, indem die Privatsphäre bereits im Designprozess berücksichtigt wird.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Abstract

There is a significant demographic shift ahead: the older population is growing in size and proportion, leading to a lack of available informal caregivers. Research has thus proposed promising technological solutions, such as care robots that enable older adults to preserve their autonomy and stay at home longer. While robotic technologies bring many advantages, they can also amplify existing problems such as the violation of privacy. This thesis aims to provide an insight into how privacy aspects related to care robots are negotiated in contemporary literature. Specifically, publications from 2010 to 2021 are analyzed using qualitative coding to find prevalent narratives and notions, as well as suggested mitigation strategies to prevent harming the users' privacy.

The body of relevant literature was gathered in a systematic literature review, which included publications on the topics of care robots, socially assistive robots, and Ambient Assisted Living (AAL) technologies. Meta-data was taken from the records, and an overview of the literature was provided. The publications which added major contributions to the research question were assessed in full-text and the contents were discussed in detail. The results show that a significant portion of the publications deal only marginally with the issue of privacy. Researchers name many concerns, among the most pressing are surveillance and the rise of Artificial Intelligence (AI) technologies in combination with big data and machine learning, which could lead to unprecedented challenges to privacy.

An abundance of mitigation strategies are discussed: transparency, informed consent, the Privacy by Design (PbD) approach, and contextual integrity are the most prevalent among them. Nevertheless, the practical application of these strategies is usually unresolved and requires further research. It was found that privacy was mostly negotiated along the informational and physical dimensions, while social and psychological privacy are not sufficiently considered. This imbalance is reflected in the discussion on concerns as well as in the proposed solutions.

In general, there is a consensus that the advantages of robotic care technologies outweigh the potential risk of violating privacy. It is recommended to proceed with caution, and act proactively rather than reactive, by considering privacy already in the design process.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Contents

Kurzfassung **vii**

Abstract **ix**

Contents **xi**

1 Introduction **1**

2 Theoretical Foundations **7**
2.1 Robotic Technologies in Care 7
2.2 Privacy 11
2.3 Emerging Technologies 16

3 Method **19**
3.1 Gathering the Literature 19
3.2 Qualitative Content Analysis Method 22
3.3 Overview of Relevant Literature 23

4 Findings **31**
4.1 Dimensions of Privacy Discussed in Literature 31
4.2 Notions on the Privacy Impact of Care Robots 34
4.3 Privacy Concerns Caused by Care Robots 42
4.4 Privacy Violation Mitigation Strategies 51

5 Future Challenges **69**
5.1 Social and Psychological Privacy 69
5.2 Use of Emerging Technologies 70
5.3 Limited Insight into Wearable Smart Devices 70
5.4 Lack of Empirical Knowledge 71
5.5 Taking Generational Change into Account 71
5.6 Engineer's Rationality? 72
5.7 Proceed with Caution 73
5.8 Other Issues that Need to be Addressed 75

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU WIEN Bibliothek Your knowledge hub

6 Discussion and Conclusion **77**

A Tables of the Literature Overview **81**
A.1 Variables 81
A.2 Results 84

B Tables of the Qualitative Analysis **87**
B.1 Codebook 87

List of Figures **97**

List of Tables **99**

Acronyms **101**

Bibliography **103**

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU WIEN Bibliothek Your knowledge hub

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

CHAPTER 1

Introduction

The older population is growing in size and proportion globally (United Nations, 2019a). In a detail report the United Nations (2019b) estimate that as of 2019, 9% of the world population was aged 65 or older, in 2030 it is projected to be over 11% and until the end of the century it is expected to double to more than 22%. In Europe and Northern America the estimates in the reports show that the population over 65 years was already around 18% in 2019, and is projected to be 26% by 2050 and close to 30% by 2100. The numbers from Japan stand out in particular, as already 28% of the population were over 65 years in 2019 (United Nations, 2019b). The trend of the ageing society can be seen for Europe in Figure 1.1, which shows the projected population of the EU-27 until 2050 by Eurostat[1]. Yamazaki et al. (2012) describe the three major problems associated with such an aging society: (i) insufficient manpower, (ii) higher cost of social insurance and (iii) more households with heavy housework burdens due to changing family structures. As the baby boomers, born between 1946 and 1964, reach late stages of their life, there will be a significant lack of available informal caregivers such as spouses and children, who play an essential role to enable elderly people to remain at home as long as possible (e.g., Redfoot et al., 2013; Ryan et al., 2012). In the United States, the ratio of available potential informal caregivers per frail older person is projected to drop from 7 in 2013 to just 4 in 2030 and to decline to 2.9 by 2050 (Redfoot et al., 2013). Consequently, Redfoot et al. argue, that with fewer informal caregivers available, the demand for institutional care as well as health care costs will rise. To counter these problems, Mitzner et al. (2010) point out that assistive technology can help to reduce the burden on family members and professional caregivers, while also increasing the independence of the elderly.

In recent years, research projects have developed such assistive technologies, that range from devices that motivate people to be physically active to devices that help to counter

[1] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Ageing_Europe_-_statistics_on_population_developments, last accessed November 30, 2021

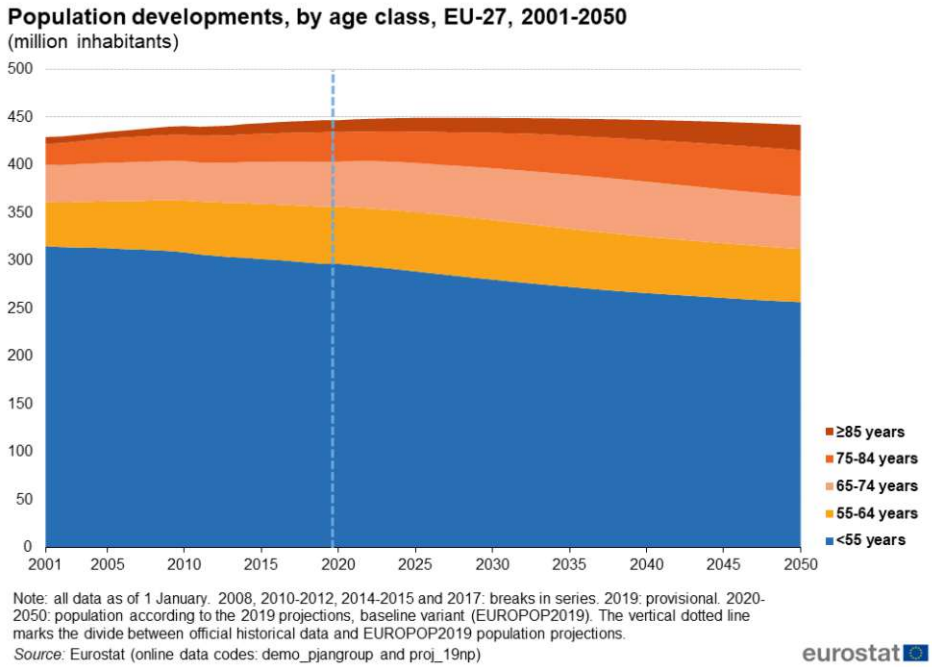


Figure 1.1: Projected population developments of the EU-27 between 2001-2050[1]

loneliness. In the following, some of those projects are briefly presented to create a comprehensible understanding of the impact on privacy such care robots may have. Fasola and Matarić (2010, 2013) show that socially assistive robots are feasible with elderly participants when they successfully used Bandit, an anthropomorphic robot platform, to engage with users and motivate them to perform physical exercises. The robot BUDDY by Blue Frog Robotics provides companionship and assists in daily activities such as by taking memos, setting timers, reminding of medication, but it is also able to detect falls or unusual inactivity.[2] A similar concept is pursued by the robot Pearl, as introduced by Pollack, Brown, Colbry, Orosz, et al. (2002), which assists elderly people in their daily activities, reminds of taking medicine, eating and drinking or using the bathroom, but it can as well help the users to navigate their environments. The projects SERROGA (Gross et al., 2015) and HOBBIT (Lammer et al., 2014) are specifically designed to provide health assistance for elderly to increase self-efficacy so they can remain living in their own homes for as long as possible. SERROGA has integrated fall detection, pulse rate monitoring as well as exercise monitoring among other functionalities, allowing elderly people to increase their self-efficacy (Gross et al., 2015). HOBBIT assists in tasks as picking up and transporting objects, emergency recognition but also in implementing fitness programs and by providing reminders to users (Lammer et al., 2014). Similarly to that, Care-O-Bot can communicate and interact with visitors, move around autonomously and handle objects with a manipulator arm to assist in the home environment (Graf,

[2] `http://www.bluefrogrobotics.com/robot`, last accessed August 6, 2021

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Hans, et al., 2004; Graf, Reiser, et al., 2009). A different approach is taken by Aido developed by InGen Dynamics, which is not specifically designed for the elderly, but still can assist significantly with household activities and remind of events to keep up a schedule, as it includes features of home automation, security, assistance as well as entertainment.[3] To keep older adults engaged and avoid cognitive decline, Furuta et al. (2012) introduced Babyloid, a baby-like robot that needs to be taken care of, to activate rational thinking and emotions, forcing the users to take a social role that helps them to recognize their own needs (Furuta et al., 2012).

In addition to such physical assistance activities, robots are also increasingly taking on social roles, as the following examples show. As more older adults live alone in their homes, social isolation and loneliness are increasing (Isabet et al., 2021). During the COVID-19 pandemic, this phenomenon has risen significantly due to lockdown measures as well as limited social exchanges for institutionalized persons (e.g., Van Dyck et al., 2020; Isabet et al., 2021; Simard and Volicer, 2020). According to National Academies of Sciences (2020) isolation and loneliness are associated with accelerated cognitive decline, depression, anxiety, lower perceived well-being and higher risk of cardiovascular morbidities among others. It is therefore that assistive technologies were developed to engage in conversations, such as the EMiR robot (Rincon et al., 2019), which is based on the RobElf[4] platform, capable of interacting with humans, detecting emotions and to recommend activities from the acquired information. The robot can classify and express the seven emotions: afraid, angry, upset, happy, neutral, sad and surprised, and by that respond empathetic towards patients needs (Rincon et al., 2019). Catalia Health's behavioral based conversational-AI platform, can create adapted conversations based on what it learned about the patient's interests and personality.[5] The platform can be deployed on the social robotic interface Mabu,[6] as well as mobile apps and web applications. There are also approaches to increase physical contact for the elderly. Wada et al. (2003) describe the seal-like robot Paro, which physically interacts with patients. The pet robot has tactile, vision, audition and posture sensors that allows it to respond when it is petted or talked to, which should stimulate the users affection (Wada et al., 2003). NeCoRo is a cat-like pet robot, expressing surprise, satisfaction, anger and hatred at human interaction, just as a real cat might do (Nakashima et al., 2010). According to Nakashima et al. (2010) the project aims to create a loving relationship to the robot to boost the user's quality of life. The Manzani robots use entertainment to fight loneliness, by performing typical Japanese stand-up comedy, traditionally performed by two comedians (Martinez-Martin and del Pobil, 2018; Umetani, Aoki, et al., 2016; Umetani, Mashimo, et al., 2014). Recent publications even discuss whether robots should be used in care for older adults or persons with disabilities to experience intimacy

[3] `https://www.startengine.com/aido`, last accessed August 6, 2021

[4] `https://www.indiegogo.com/projects/robelf-your-mobile-monitoring-robot`, last accessed August 6, 2021

[5] `http://www.cataliahealth.com/platform-ai`, last accessed August 6, 2021

[6] `http://www.cataliahealth.com/introducing-the-mabu-personal-healthcare-companion`, last accessed August 8, 2021

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

and sexual pleasure (Eduard Fosch-Villaronga and Poulsen, 2021; Jecker, 2021). But technologies to decrease loneliness do not necessarily have to be humanoid or animal-like robots, as will be explained in the following. KOMP is a tool that allows seniors to reduce loneliness by keeping in touch with family members with today's available communication technology while offering a simple user interface leaning on the minimalist design of radios or TVs from the 1960s to overcome the technology barrier.[7] But even apart from such research projects, there are already virtual assistants widely spread in our homes. During the COVID-19 pandemic, the BBC reported how AI based voice technologies, such as Google Home smart speakers, could help to combat loneliness of elderly people.[8]

In the introduction to this thesis it was established that there is a need for assistive technologies due to a shift in the ratio of the older persons to potential caregivers. Moreover, the requirements for the technology were defined by discussing the existing approaches: they should be able to assist patients physically, they might need to be controllable by voice, thus also understand and be able to give answers, and they need to sense their surroundings, to interact with the patient. Traditionally, most of these tasks were performed by informal caretakers, which mostly were family members. While sharing intimate information or situations with informal caregivers might be uncomfortable in some situations, the impact privacy of the patient is limited, as there are no recordings or other unwanted large scale information disclosures of the patient. When assistive technology are used as a replacement or additional help, intimate situations and information might be shared with a company, private individuals or a government somewhere around the globe. The potential problems of such sharing of sensitive data becomes clear when considering scandals involving the infringement of privacy. Recently the scandal around the Pegasus spyware (e.g., Marczak et al., 2018) became known, which allows a private company to spy on citizens around the world via their iOS or Android or mobile devices. Amnesty International calls this a violation to human rights.[9] Robots could significantly expand the possibilities for spying; in addition, sensitive health data is shared with care robots over the Internet, which is not currently possible on this scale.

To examine the actual impact on privacy, it is first necessary to delineate what privacy is and what technologies are examined. Burgoon (1982) introduced four dimension of privacy: physical, social, psychological, and informational. With social robots, all of the four dimensions are affected. They have the ability to move in personal space, thus affect physical privacy, collect and process data, thus affect informational privacy. Furthermore, people who interact with robots can build up an emotional and social connection, which affects psychological and social privacy. The purpose of this thesis is to show how the privacy impact of care robots is negotiated by contemporary research. provide an overview

[7] https://www.noisolation.com/assets/documents/How-and-why-we-made-KOMP-1.pdf, last accessed August 6, 2021

[8] https://www.bbc.com/worklife/article/20200325-can-voice-technologies-using-ai-fight-elderly-loneliness, last accessed August 6, 2021

[9] https://www.amnesty.org/en/latest/news/2021/07/pegasus-project-spyware-digital-surveillance-nso, last accessed August 10, 2021

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

of the research conducted on the privacy impact of care robotics. Chapter 3 gives an overview of the relevant literature, while the contents of the most relevant contributions are discussed in Chapter 4. In Chapter 5 research gaps and challenges that need to be addressed in the future are pointed out. These objectives form the basis for the research question.

Research Question

RQ: How does current literature consider the impact on privacy by care robots, socially assistive robots or ambient assisted living technologies?

- **RQa**: What, where and by whom has been published?
- **RQb**: How is privacy currently being negotiated in science?
- **RQc**: Which questions have to be addressed in the future?

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU WIEN Bibliothek Your knowledge hub

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

CHAPTER 2

Theoretical Foundations

2.1 Robotic Technologies in Care

The literature review will include publications on Ambient Assisted Living (AAL) technologies, care robots and and wearable devices. This classification is similar to the study by Ienca and Eduard Fosch-Villaronga (2019), which inspect privacy related aspects of these three care technology types. Nevertheless, it is also common for those technologies to occur in combined form, for example when a mobile robot navigates through a room using stationary sensors, or when measurements such as pulse rates are transmitted from wearable smart devices to other systems.

2.1.1 Ambient Assisted Living (AAL) Technologies

Ambient Assisted Living (AAL) technologies are stationary systems based on information and communications technologies (ICT) that help older adults or other persons in need of assistance to handle certain tasks related to their health, that allow them to gain autonomy and enable them to stay at home longer. AAL technologies are composed of a network of sensors, that can detect fires, running water, if a stove was left on, if doors are left open and also due to their possibilties of sending signals they can warn users.[10] Figure 2.1 shows the concept of an AAL system, which points out the different possible sensors and signalling solutions, as well as the involved actors, that range from the patient, to the care personal to the first responders. The involved actors are all cross-linked by the central role of the AAL system. In the figure the AAL system is represented by a robot, nevertheless this can be misleading as those system are actually not mobile, as a robot would suggest. Example applications are to monitor using cameras and to detect life threatening situations by algorithmic decision making (Muñoz et al.,

[10] https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Artikel/UseCases/smart-living-aal.html, last accessed November 23, 2021

2011), next to fall-detection they also can be used to detect exceptional inactivity with distributed multi-camera vision (Aghajan et al., 2007). Nevertheless, they also help with rather simple tasks such as to remind older adults in cognitive decline of taking medicine or on other routine tasks (Pollack, Brown, Colbry, McCarthy, et al., 2003). Moreover, AAL technologies can alert caregivers or other medical experts in case of emergency (Eklund et al., 2006), and generally can be used to monitor the health conditions at home, to assist medical experts and avoid unnecessary transports to hospitals (Figueredo and Dias, 2004). They furthermore can assist in other cognitive tasks such as guidance in order to preserve mobility (Dubowsky et al., 2000), and help to reduce loneliness – consequently the technologies can impact health and quality of life positively by staying socially connected to family and friends (Pensas et al., 2014). Smart speakers, such as Amazon's Alexa, Google Home or Apple's HomePod are already a form of assisted living, as it is possible to use them for ordering groceries, make phone calls and in combination with other smart home devices control certain aspects of a house, such as temperature, with voice commands; also they can be linked to smoke detectors or detect running water. While not optimized for older people, such smart speakers and connected privacy impacts shall therefore be considered as well if they are accounted for in the body of literature. It was also reported that during the COVID-19 curfews and contact restrictions, some older adults were using smart speakers as a means to combat loneliness.[8] While the possibility can not be excluded, it can be expected that AAL systems are less likely to be attributed social properties due to the lack of an anthropomorphic physical existence.

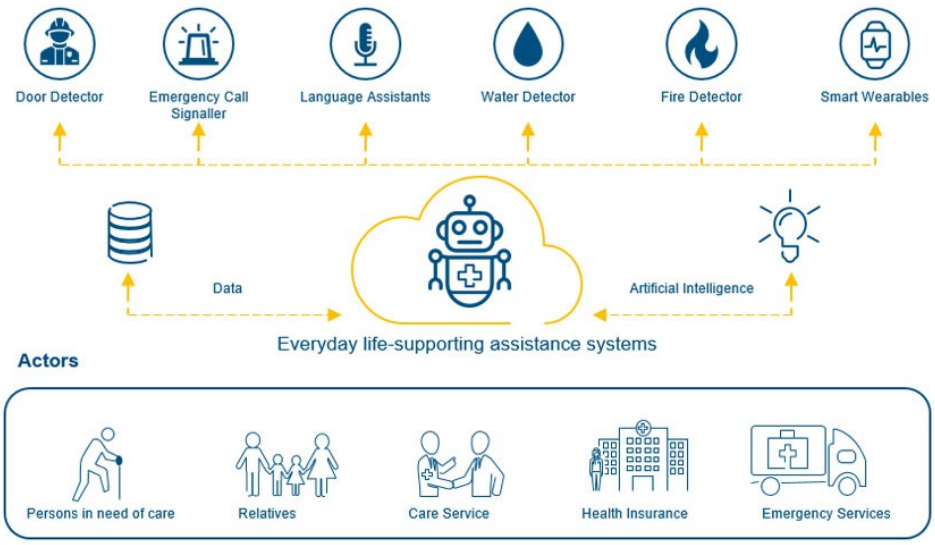


Figure 2.1: Concept of an Ambient Assisted Living (AAL) system by the GAIA-X project[10]

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

2.1.2 Care Robots

Care robots differ from AAL technologies in their ability to move around the space, manipulate their environment, and also physically interact with the patient. They can be fully autonomous or semi-autonomous. The robots fulfill similar tasks as AAL when it comes to detection of emergency situations such as a fallen person, or when medical personnel should be notified (Armbrust et al., 2011). Furthermore they are used to monitor (Van de Ven et al., 2010) and assist to connect with family and friends (Casey et al., 2016). One major difference to AAL technologies is that robots are not stationary and thus they can also perform household tasks, lift objects and actively assist older people with their mobility (Graf, Hans, et al., 2004). They can be used to lift physically impaired patients e.g., from a wheelchair to a bed (Mukai et al., 2010) and not insignificantly, they can also provide companionship (Martinez-Martin and del Pobil, 2018). Another advantage of mobility compared to a stationary AAL system, is that sensors do not need to be installed in every room of the living space, as the robot can freely move around e.g., to perform monitoring tasks (Van de Ven et al., 2010).

At this point, a distinction must be made as to what is included in the literature research as a care robot for the purposes of this thesis. The following definitions of different robots used in care will serve this purpose. ISO 8373:2014 defines different types of »personal care robots« (ISO 8373:2014, as cited in Jacobs and Virk, 2014):

- *Mobile servant robots*: They can assist with tasks, manually or informative; they can work in the private household or in public areas.
- *Person carrier robots*: The essential task is the transportation of people.
- *Physical assistant robots*: Robot technology which is attached to the body of the patient to support mobility, e.g. exoskeletons, but also walking aids such as robotic walking frames.

Moreover, Feil-Seifer and Matarić (2011) define Socially Assistive Robots (SARs) as the intersection of *assistive robots*, which are characterized by the fact that they support patients in certain tasks (e.g. mobility), and *socially interactive robots*, which have the ability for social and nonphysical communication. Therefore, a SAR could be either of the types defined in ISO 8373:2014, if the respective personal care robot has the additional capability of social interaction. Combating loneliness is important in a care context, as it can lead to health conditions such as cognitive decline, depression but also high blood pressure (Isabet et al., 2021).

Social robots, on the other hand, are merely supporting in a home environment in a natural interaction, by performing tasks such as to inform about the weather or news, to schedule and remind of appointments, or notify contacts in case of an emergency (Heuer, Schiering, and Reinhardt Gerndt, 2018). In the the analysis also publications on social robots were included, as arguably many of the challenges they face regarding privacy can

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

be applied to (personal) care robots as well – presumably while the latter are dealing with more privacy sensitive information such as health data.

Telepresence robots allow a person (e.g. healthcare personnel) to control a mobile robot in the living space of a patient, to physically and socially interact with a patient (Gonzalez-Jimenez et al., 2013). A sub-category of telepresence robots, are *social telepresence robots*, which are specifically used to combat loneliness among patients (Isabet et al., 2021).

(a) Service robot Care-O-bot 4 by Fraunhofer IPA[11]

(b) Socially assitive robot Misty II by Misty Robotics, Inc.[12]

(c) Telepresence robot Double 3 by Double Robotics, Inc.[13]

Figure 2.2: Three examples of care robots with different approaches: (a) a service robot, (b) a socially assistive robot and (c) a telepresence robot

To gain as complete an understanding as possible of the influences on privacy by care robots, all of the aforementioned robot types will be considered in the literature review: Mobile servant robots, person carrier robots, physical assistant robots, social robots, Socially Assistive Robots (SARs), telepresence robots. In Figure 2.2, some examples of the robots mentioned are presented, although it is important to point out that this representation does not include all variations. It can be expected that the different types of robots described in this sections will have different impacts on privacy, for example an exoskeleton may have less personal knowledge about a patient than a social robot which is entrusted with intimate secrets; however, it can also be assumed that many of the solutions offered are hybrid variants, combining physically assistive tasks with social tasks.

[11] `https://www.care-o-bot.de/de/care-o-bot-4/download/images.html`, last accessed November 23, 2021

[12] `https://www.mistyrobotics.com/use-cases/misty-ii-a-partner-in-socially-assistive-therapy`, last accessed November 23, 2021

[13] `https://www.doublerobotics.com`, last accessed November 23, 2021

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

2.1.3 Wearable Smart Devices

Wearable (smart) devices include smart watches, wristbands, other wearable mobile sensors and mobile medical devices (Dinh-Le et al., 2019), among others they can measure blood pressure, heart-beat rates, sugar levels to just name some of the physiological and health-related parameters (Ienca and Eduard Fosch-Villaronga, 2019). Kumar et al. (2013) also include mobile phones in their definition of mobile health technology, as they have sensors and can be used for tracking daily activities. The combination of multiple sensors with the Internet of Things (IoT) approach can also be used do detect anomalies when monitoring the health condition of patients (Yan et al., 2015). The measures should assist medical staff to make decisions, and thus improve health outcomes (Kumar et al., 2013). Privacy is already an important aspect discussed for wearable health devices, as the collected patient data is currently mostly processed by third parties, such as Apple Health, Google Fit, Fitbit, Nokia, and Withings (Dinh-Le et al., 2019). In some cases, it is also possible that the wearable devices are manufactured by different companies, while the data is processed in a software by another provider, as can be seen in Figure 2.3, showing the concept of Technosoft Solutions;[14] furthermore many third party apps or devices offer integrations for Apple Health and Google Fit (Dinh-Le et al., 2019).

Figure 2.3: Integrated solution for wearable health technologies by Technosoft Solutions[14]

2.2 Privacy

Before analyzing the different perspectives on the privacy impact of care robots, it is necessary to understand the concept of privacy. Despite the fact it is common to use the term in different situations in everyday life, there is no generally accepted definition of privacy. One of the oldest definition comes from Brandeis and Warren (1890), calling it simply the »right of the individual to be let alone«. Schoeman (1984) recites other definitions that were proposed as (i) one's right to decide which information about oneself is shared with others, (ii) a measure of control – over information, personal identity

[14] `https://techno-soft.com/wearable-technology-in-healthcare.html`, last accessed November 23, 2021

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

or physical access concerning oneself, and finally (iii) a state of limited access to an individual. Those definitions include an informational aspect, a physical aspect, in the sense that a person should have control whether some other entity or person should have access or influence to the physical space in proximity of the individual, but also adds an aspect of intellectual property, by granting the control over one's identity. Privacy International defines privacy as concept that helps to establish boundaries in order to limit who has access to the our bodies, places and things, as well as communications and information;[15] which is a definition that includes territorial claims the body and the place (such as the home), property rights, in the sense of owning things but also the right to private communication (intellectual property) and information, which implies the control of information about oneself. Control over one's physical space (home), intellectual property (honor and reputation) and information (arbitrary interference) is also formulated as a human right, as the Universal Declaration of Human Rights (UDHR)[16] (Article 12) states:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks. (Universal Declaration of Human Rights, Article 12)

Whether storing, sharing and handling personal information about an individual is »arbitrary interference«, – or formulated in another way, to which extend those actions would be acceptable –, is not further specified in the Universal Declaration of Human Rights (UDHR). The European court of human rights is one step ahead when it comes to the informational aspect of privacy. The right to privacy is defined in the European Convention on Human Rights (ECHR),[17] (Article 8) under the title »*Right to respect for private and family life*«, and lists the following points:

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.
>
> (European Convention on Human Rights, Article 8)

According to Koops and Leenes (2005) these points as defined by the ECHR refer to three dimensions of privacy protection measures: (1) physical privacy, the protection of one's

[15] `https://privacyinternational.org/explainer/56/what-privacy`, last accessed August 23, 2021

[16] `https://www.un.org/en/about-us/universal-declaration-of-human-rights`, last accessed August 22, 2021

[17] `https://www.echr.coe.int/Documents/Convention_ENG.pdf`, last accessed August 22, 2021

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

physical body against unwanted medical procedures, but also the prevention of intrusion into the home among others; (2) relational privacy, referring to the security and privacy of communication means; (3) informational privacy, which includes the collection, secure storage and handling of personal data and the like. While the European definition is very specific on the nature of what interference is acceptable or not, it leaves out the aspect of the protections against attacks on honour and reputation that the UDHR has defined. Also missing in both, the UDHR and the ECHR, is the aspect of the right to control one's personal identity, which Schoeman (1984) mentioned – as arguably the protection of personal information and personal identity differ. Combining all these aspects of privacy into one definition is not an easy task. It has already been established that privacy has several dimensions, but a very comprehensive description of the concept of privacy was formulated in the publication of Burgoon (1982), which is considered in detail in the following.

2.2.1 Privacy in Four Dimensions

Burgoon (1982) wrote a comprehensive analysis on the four dimensions of privacy she has identify, namely (i) physical, (ii) social, (iii) psychological and (iv) informational privacy. In the following sections each dimension is considered in detail. For every dimension examples for states of either having the maximum or the minimum possible amount of privacy are given as Burgoon formulated them. At the same time, it will be discussed why the dimensions are relevant in the context of care robots and therefore deserve attention.

Physical Privacy

The analysis starts by examining (i) physical privacy, which Burgoon (1982) describes as »the degree to which one is physically inaccessible to others«, which is similar to what Brandeis and Warren (1890) meant by calling privacy the »right of the individual to be let alone.« Whether a person wants to live in total isolation from other people, which would be as Burgoon points out the most extreme form of being inaccessible and thus total physical privacy, or to which degree other people should be allowed to interfere with ones physical privacy, again reflects the aforementioned control over physical space. Burgoon (1982) makes (a) spacial distinction between home territory, which is controlled through physical barriers, and the body territory, which is the body itself; and (b) a qualitative distinction, namely the privacy to repose, meaning the right to avoid annoyances or distressing events and the privacy to of sanctuary, referring to a physical refuge free from surveillance of others. In both discussed human rights declarations the right to ones privacy at home is mentioned in context with the family, which seemingly have a different impact on the disturbance of physical privacy than strangers. This view is reinforced by Burgoon, who finds that those who are held in highest esteem, such as friends and relatives pose the least threat to privacy violation; at the same time, those held in the lowest esteem, such as servants or service personnel, also pose less threat to privacy as they can be treated as nonperson (Sommer, 1969, as cited in Burgoon, 1982). Both of these aspects are highly relevant in the context of care robotics: on the

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

one hand, a care situation, especially in elderly care, often involves informal caregivers – mostly relatives –, who according to the before mentioned view would pose little threat to physical privacy; on the other hand, a robot, by current definition, is a nonperson, with no rights and therefore deemed property and bound to serve the caretaker, and thus would mean no harm in terms of privacy perception – if assuming that there is no third party involved capable of intercepting the sensory capabilities and spacial movement. Burgoon (1982) argues, it is the individuals in the center field, between those held in high esteem and those who can be regulated to a nonperson status, which are perceived as the most disturbance to physical privacy.

Social Privacy

The second dimension (ii) social privacy, which can be expressed in simplified form as the control over one's interactions. Burgoon (1982) defines four degrees of control in regards to interaction, (a) control over who the participants are, (b) control of the frequency, (c) control over the length and finally (d) the control over the content, and distinguishes between being reserved or intimate, where the former would reduce the number and frequency of interactions and the ladder would maximize knowledge and personal information among one and another. Naturally, Burgoon argues, a persons openness to interaction and conversation would also change by mood, condition on a particular day, and the type of interaction among other factors, e.g. a situation such as a job interview compared to a meeting with friends will be perceived different by a person. Burgoon (1982) argues, one would interact on a formal level in a job interview, which strengthens the individuals ability to maintain reserved, while among friends the informal nature of the interaction invites for longer and more frequent contacts. With regards to care robots, the degree of formality in the conversation is an engineering design choice, which as an inference can directly influence the perceived violation of social privacy. Remarkably, Burgoon (1982) found that social privacy is not limited to a single individual, but can also be applied to a group state, meaning that a set of close persons can form a social bubble that excludes the outside world, while experiencing no invasion of their individual social privacy, such as a couple having dinner in a restaurant are forming their own social group. This narrative certainly would also allow social groups, where members are nonhuman social robots, capable of advanced interaction. While the differences between physical and social privacy are undeniable, Burgoon (1982) finds that often a motivation to achieve physical privacy is the social privacy that accompanies it, which consequently means that if an individual or group loses autonomy – the ability to make decisions and act independently –, it always poses a threat to social privacy as well. Naturally, social robots have the ability to interact with humans, which will affect the aspects of social privacy mentioned.

Psychological Privacy

The third dimension of privacy (iii) psychological privacy, can be seen as the right to protect intellectual private property (Simmel, 1950, as cited in Burgoon, 1982). While

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

related to social privacy, psychological privacy can be regarded as a separate aspect, which allows to create boundaries between the self and other persons, which shapes the self-definition and the definition of relationships to others and thus allows the freedom from the influence of others on one's thoughts and feelings (Burgoon, 1982). The self-definition aspect of psychological privacy, Burgoon finds, correlates to the definition of Schoeman (1984), which includes the right to control the personal identity. Burgoon (1982) continues to argue that psychological privacy is connected to physical and social privacy, as the lack of possibility to retreat physically and/or socially, compromises the sense of identity. Psychological privacy can, according to Burgoon, also be seen as the opportunity to interpret and internalize the comparison of oneself to other persons, which helps to shape present and future actions. This raises the question if the presence of a robotic caregiver could influence one's sense of identity – as one would compare oneself to the robot. Moreover, Burgoon argues that the level of how psychological privacy is experienced, is connected to the degree of physical and social privacy an individual can achieve: the extreme forms are being free of any external interference or to be subjected by brainwashing (Burgoon, 1982). Social robots, if not considered carefully, open up the possibility of constant bi-directional information exchange; meaning on the one hand they can collect information about one's identity, on the other hand the robots actions might influence the identity of the user – in extreme cases brainwash them – by providing biased information. Learning a persons secrets and penetrating the inner zone, would leave a person vulnerable to ridicule and shame, and shift the control over oneself to those who know one's secrets (Westin, 1970, as cited in Burgoon, 1982). Finally, according to Burgoon (1982), the optimal level of stimulation by one's physical surroundings is the intermediate of excessive stimulation, which can distract and annoy, and under-stimulation which would lead to deprivation and the desire for more human contact. To avoid excessive stimulation could pose a challenge if a care robot must be continuously present to ensure a patient's health and safety.

Informational Privacy

The fourth dimension (iv) informational privacy, considers information about a person, group or organization, which is gathered and spread without their knowledge, and thus lies beyond the control of the individual in question (Burgoon, 1982). This aspect of privacy is often discussed in regards to emerging technologies, as especially digitization allows the processing of large amounts of personal information in forms of databases, and such data is the basis for machine learning applications – which are often incomprehensible for humans. Burgoon (1982) was already pointing out in 1982 that computers and data storage potentially involves challenges such as poorly developed legal restrictions, risks due to tapping into data bands, human errors in data entry or inaccurately or maliciously reported information; and furthermore, Burgoon mentioned, that those technologies were in the past and will be in the future used for illegal wiretapping, searches and seizures, espionage by governments, industry or otherwise politically motivated entities. This shows the core aspect of informational privacy, namely that the degree of control over the data is what defines it. Burgoon (1982) describes the considerations whether an

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

individual perceives a threat to one's informational privacy as follows: (a) to what degree can the individual exercises control over the release and distribution of data, (b) the amount of information out of one's control, (c) the number of persons having access to said information, (d) the content of the information and finally (e) the relationship the individual has to those who possess the information. This is in accordance with the definition by Schoeman (1984), which grants the individual the agency of which information is shared with others and also gives the control over this information. The Universal Declaration of Human Rights (Article 12) emphasizes especially the »protection of the law against such interference or attacks«, which in context of informational privacy means the protection against spying and unwanted distribution of personal data. The ECHR (Article 8) more specifically names the exceptions to this protection, which not exclusively, but as well relates to the informational aspect of privacy. Thus, it seems that there is also a willingness or at least no opposition of individuals to share data: for example with government organizations. Burgoon (1982) finds that the knowledge of one's age, educational records etc. poses less violation to privacy than on one's sexual habits, political information or financial situation. On the other hand, Burgoon brings up an interesting exception: the »stranger-on-the-bus phenomenon«, when an individual is willing to share highly intimate information to total strangers – a person that one is not expecting to ever see again –, as due to the anonymity of the situation there is not perceived loss of informational privacy (Simmel, 1950, as cited in Burgoon, 1982). A social robot could be perceived as a stranger, or one could imply that a machine does not understand the shared information anyways, thus creating a sense of anonymity – encouraging persons, unintentionally or intentionally, to share intimate information. Finally, Burgoon (1982) defines the extreme conditions of informational privacy as, (a) total anonymity accompanied by freedom of expression and no misuse of one's data, and (b) being a public figure, where information is actively gathered and publicized, and having little to no control over how it is spread and used.

These four dimensions of privacy, although interrelated, provide a fitting framework for further analyses of the privacy impact of care robots. Each of those dimensions are affected in different ways, but reactions of individuals to breaches or violations of privacy, are similar: as Burgoon (1982) summarizes, the lack of privacy can lead to stress and the related physical reactions such as anxiety, illness, feelings of helplessness, loss of self-identity and other psychological responses, to name a few. It is therefore, that privacy is formulated as a human right, and the protection of such must be ensured also in technological applications – especially if all four dimensions are affected, which is the case for care robots.

2.3 Emerging Technologies

In the following, definitions of emerging technologies which are often addressed in the context of care robots and privacy, and thus are prominently featured in this thesis, are given. Some of those technologies do not yet have final formal definition. Nevertheless, emerging technologies are important to consider in relation to privacy

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

aspects, because they can often process large amounts of data, and often do so in ways that are incomprehensible to humans. In addition, regulations on these technologies are very vague, and the constant and rapid development makes it difficult for regulations to keep pace.

- There is no final definition for what *Artificial Intelligence (AI)* exactly is, but Kok et al. (2009) list the following: (i) Machines that engage in human-like thought processes, (ii) when a machine can learn, adapt and correct itself, (iii) the extension of human intelligence through a computer, (iv) if a computer imitates intelligent human behavior.
- *Machine learning* is meant when a computer simulates human learning activities, self-improves it's methods to gain new skills and new knowledge as well as to improve it's performance constantly (Wang et al., 2009). Machine learning is used in combination with Artificial Intelligence (AI) algorithms.
- *Deep learning* is when an machine learning algorithm does not only learn the relations of several variables, but gathers also the knowledge that makes sense of the relation (W. Zhang et al., 2018). Deep learning therefore can understand and create knowledge which might be incomprehensible for humans.
- The *Internet of Things (IoT)* is a comprehensive combination of physical and digital components to create novel products (Wortmann and Flüchter, 2015). Essentially, products that might already be available will be equipped with the possibility to be connected to the internet in the future, as for example was the case when conventional TVs were upgraded to become smart TVs.
- *Big data* is when AI algorithms can make sense from large amounts of data, which would be otherwise not possible for humans. There is a formal definition provided by De Mauro et al. (2016): »Big Data is the Information asset characterized by such a High Volume, Velocity and Variety to require specific Technology and Analytical Methods for its transformation into Value.«
- *Cloud computing* is meant, when the actual computing operations are not performed on local devices. »Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.« (Mell and Grance, 2011)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU WIEN Bibliothek Your knowledge hub

CHAPTER 3

Method

This chapter describes the method for gathering the body of literature for the literature review. Furthermore, it is outlined how the qualitative contents are evaluated, which are discussed in detail in Chapter 4. Finally, in Section 3.3 an overview of the relevant literature on the privacy impact of care robots is given. This shall provide an overlook through which lens members of different academic disciplines approach the topic, in which geographic regions it is discussed and in which journals or conferences. This bibliographical overview is intended to provide an understanding on the underlying motivations of the authors for publishing on the topic and thus provide an answer to **RQa** ("What, where and by whom has been published?").

3.1 Gathering the Literature

The methods for literature reviews described by Xiao and Watson (2019) were adapted to perform the analysis in this thesis. To begin with, the relevant body of literature has to be found by searching available databases. Figure 3.1 shows an overview of the method used for the literature review.

Database search A total of 333 publications were retrieved from Google Scholar and 1 from Google by using the search terms listed in Table 3.2. The general settings of the online databases can be seen in Table 3.1, notably only English-language articles were included for the review. Also the search was reduced to only include articles from 2010 to mid 2021, when the literature search was conducted. Older publications were not included, as the technologies have changed radically ever since smartphones dominated over conventional mobile phones and computing became more ubiquitous. Moreover, social media certainly raised more challenges regarding privacy. Articles published prior to 2010 were included, if they seemed to have high relevance as they are referenced often in other publications and nevertheless were close to the publishing date of 2010. To

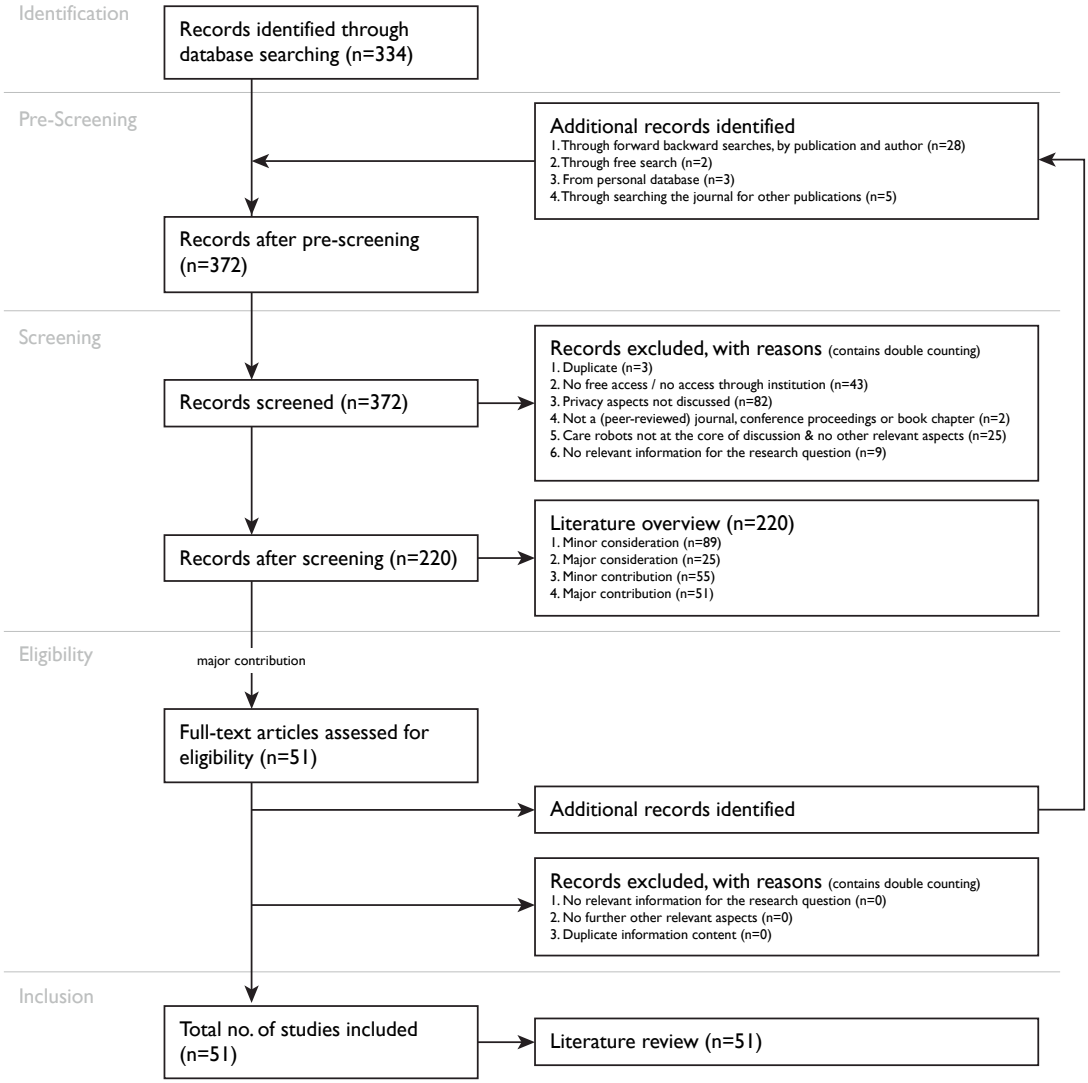


Figure 3.1: Method of the literature review, adapted from methods used by Vandemeulebroucke, de Casterlé, et al. (2018) and Xiao and Watson (2019)

narrow down the results to the most promising publications, logical operators, quotes and parentheses were used. Both Google Scholar and Google allow using AND ($\wedge$) to ensure that multiple phrases need to be included, OR ($\vee$) if any of the variation of a search term have to be included. Quotes ("search term") can be used in order to make sure the term is included exactly as written, and parentheses allow groupings of conditions. The search strategy is summarized in Table 3.2, where the search strings are split into groups of »Robotics« and »Privacy or Ethics«, which are coupled with a logical AND operator to ensure both are included in the articles of the search results.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Database	Settings	
All databases	**Language:**	English-language articles only
Google Scholar	**Find articles:**	With **all** of the words
	Where my words occur:	**Anywhere** in the article
	Return articles **dated between:**	2010 - 2021 (now)

Table 3.1: Database search settings

Database	Included (for screening)	Date	Search			Results
			Group **Robotics**	∧	Group **Privacy** *or* **Ethics**	
Google Scholar	333	Aug 5, 2021	care robots		privacy	About 24,700
		Aug 5, 2021	("care robot" ∨ "care robots")		privacy	
		Aug 5, 2021	("assistive robot" ∨ "assistive robots")		privacy	About 4,940

Table 3.2: Database search terms and results

Pre-screening As the databases Google Scholar and Google provide a large abundance of results, the publications had to be selected according to the relevance of their respective title and the preview text shown. The inclusion criteria for the screening process are listed in Table 3.3. It is apparent that despite applying these inclusion criteria, many of the records will not have relevance for the research question – therefore exclusion criteria were defined in the screening process.

ID	Inclusion criteria: Screening
1	Title of the record suggests relevance to the research question
2	Record is not older than 2010 (exemptions for records that are cited often in other publications)
3	Record appeared in a peer-reviewed journal, conference proceedings or as a book chapter
4	Record is written in English

Table 3.3: Criteria for the inclusion for the screening

Screening In the screening procedure, 131 of the overall publications retrieved from the online databases were excluded for reasons which can be seen in Table 3.4. As some publications were excluded for several reasons, the numbers in the table include double counting. Despite the narrowing down in the search terms, that all publications should at least include the term »privacy«, a total of 82 publications have been removed due to the total absence of the term or without discussing it in the slightest. While the Google Scholar database search delivered very relevant publications, in the later results the algorithm apparently also shows entries while skipping the mandatory inclusion of the term »privacy«. Another explanation for results showing up but not including the term »privacy« could be that the search also includes other segments of the website where the publication is hosted, and thus would included the »privacy statement« in the search which is present on most websites. Duplicate entries that were retrieved in the database search were also removed. If a citation for a book was included, but also one or more book chapters of the same book written by different authors, only the respective

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

chapters were kept and counted as a publication each.

ID	Records excluded, with reasons	No. of publications (contains double counting)
1	Duplicate	3
2	No free access / no access through institution	43
3	Privacy aspects not discussed	82
4	Not a (peer-reviewed) journal, conference proceedings or book chapter	2
5	Care robots not at the core of discussion & no other relevant aspects	25
6	No relevant information for the research question	9

Table 3.4: Records excluded, with reasons

Taking meta-data After the screening of the records, a total of 203 publications were included for the overview of the relevant literature. In this stage the contents of each included publication was analyzed on a superficial level, to create and collect the relevant meta-data. A list of parameters that were taken into account can be found in Tables A.1 to A.3 with detailed descriptions. While screening the contents of the publications for key words such as »privacy«, »health«, »care« or »robots«, the general approach to the topic of care robots was found, and this brief inspection of the documents also helped identifying further relevant literature. Thus, another 10 publications were included through backward and forward searches, meaning studies that were referenced in the the record (backward), or other publications that referenced to the record (forward). Furthermore, if an author had published several interesting papers, the past (backward) and future (forward) publications of the author were screened as well. Moreover 3 records were included by inspecting other publications in the same journal, conference proceedings or book. A remainder of 1 publications were included by performing free searches in databases and 3 records were included from personal databases. The meta-data was documented in a spreadsheet, which was exported in CSV-format, so the statistical processing could be performed with iPython notebooks.

Eligibility As a final step the full-text of the publications classified as »major contribution« in regards to discussion the privacy impact of care robots were assessed for eligibility, meaning if the results add qualitative content to the research question. In this process, exclusion criteria were also defined (see Figure 3.1), nevertheless no records were excluded. Moreover, the assessment of the full-text was accompanied by a method for analyzing the qualitative content of the publications which is described in Section 3.2.

3.2 Qualitative Content Analysis Method

The qualitative part refers to those papers that were classified as »major contributions« to the topic of privacy impact of care robots in the previous screening (see Figure 3.1). The n=51 publications were examined in detail to determine (i) how and along which dimensions privacy is negotiated in relation to care robots, (ii) what problems, concerns

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

or threats are identified, and (iii) what solutions are discussed or actually proposed as technical solutions.

In order to obtain a structural understanding how these topics are are approached, the coding method was used (e.g., Saldaña, 2013). The advantage of this method is that it not only shows which topics are discussed in which publications but also makes it possible to quantify how often certain topics and approaches are discussed in the overall publications. Therefore, when analyzing the publications, so-called »codes« were assigned to specific passages or underlying ideas. Saldaña (2013) define a code as follows: »A code in qualitative inquiry is most often a word or short phrase that symbolically assigns a summative, salient, essence-capturing, and/or evocative attribute for a portion of language-based or visual data« (p.3). In this literature review, because the coding method is not applied to, say, interviews, the underlying ideas are often very obvious, such as when an author points to Privacy by Design (PbD) as a problem-solving measure which should be applied to care robots. While certain ideas are used up more often within a publication, they are only counted one time per publication for later comparison. Thus, concerns as well as problem solutions can be analyzed across all »coded« publications in this literature review. The codes used were summarized in a so-called »codebook«. The codes emerged during the full-text assessment of the publications and the codebook was continuously expanded. In the process, some of the codes then appeared as particularly relevant, while others, which occurred only rarely among the publications, were less relevant. In order to make the assignment of codes comprehensible, the name of the code, a description, and an example of the application were documented, based on the suggestions by Mihas and Odum Institute (2019). The resulting codes were summarized in the codebook Tables B.1 to B.9, whereas the tables only contain codes that were assigned more often than once, in order to improve clarity and maximize relevance. Furthermore, it was documented in which publications the described codes were applied. The coding itself was performed via highlighting directly in the PDF version of the publications, and the codes were were documented in a spreadsheet. From there, they were exported as CSV-file which was used in an iPython notebook to perform the statistical analysis.

3.3 Overview of Relevant Literature

This section provides an overview of the relevant literature considering privacy aspects of care robots, including minor as well as major contributions. The numerical results are summarized in Tables A.4 and A.5. The most interesting aspects of this bibliographic analysis are discussed in the following. It is important to study the variables defined in Tables A.1 to A.3 to understand the terminology used and displayed in the graphs.

3.3.1 Level of Contribution

Out of the 220 publications that were analyzed, 89 (40.5%) were identified to only considerate privacy in a minor way, such as mentioning it briefly or discuss it in a few non essential sentences. At the other end of the spectrum are 51 (23.2%) publications that

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

add a major contribution to the topic of privacy in care robotics. The publications that lie in-between those ends either contribute some minor aspects or considered the privacy impact thoroughly by reviewing literature but not adding new aspects. The distribution, which can be seen in Figure 3.2, indicates that articles which are not directly approaching privacy issues with care robots, for the most part do not consider it extensively. It can therefore be shown that a large number of publications on care robots and related technologies only have minor considerations on their privacy impact. It is noteworthy that from the publications that were considered in the pre-screening, already 82 had to be excluded, as they do not discuss privacy, or just very little. If one takes into account the fact that the search results already were narrowed down by the search terms, which included »privacy«, it can be expected that there is a large number of publications on care robots that do not consider privacy aspects at all. The results shown in the Figure 3.2 only includes the publications which discuss privacy in one or another way.

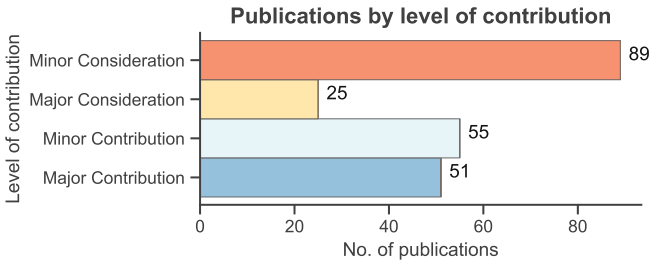


Figure 3.2: Publications by level of contribution

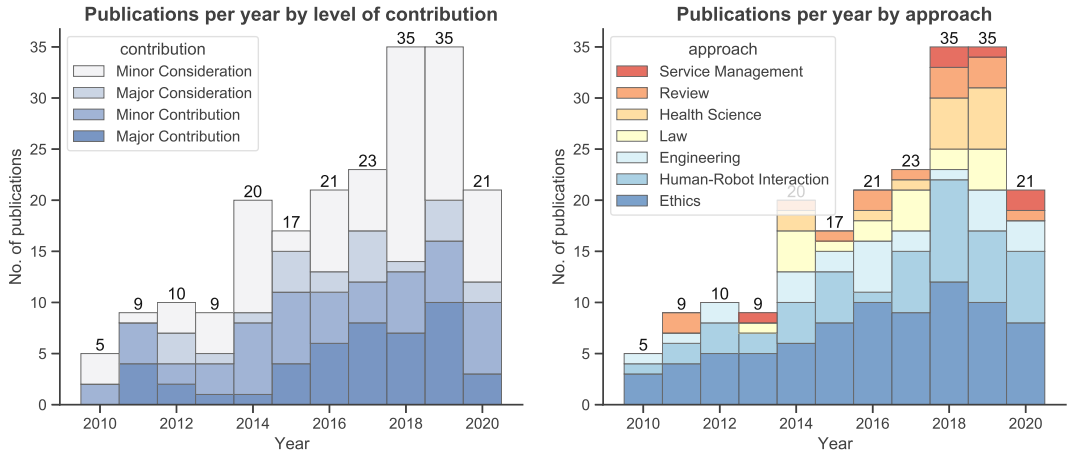
Frequency of Publications

Figure 3.3 shows the number of publications per year between 2010 and 2020. Despite limiting the database search to results published after 2010, some publications from 2009 were included as they add value to the discussion. Records from 2021 were not included in the graph, as of the time of the literature review the year was not over yet, which would distort the outcome of the graph. Overall there is a tendency for a rise in publications about care robots that consider the aspects of privacy up until the year 2019. In Figure 3.3a it can be seen also that the number of publications with minor consideration on privacy aspects have risen particularly in 2018 and 2019. The number of publication that are considered as major contributions, also rises in general up until 2019. The GDPR[18] was originally published in April of 2016 and had to be implemented in national law of each EU member state by May 2018. While the General Data Protection Regulation (GDPR) is a regional regulation, it certainly had impacted the views on privacy for researchers around the world. The sudden rise of publications, that consider privacy, between 2017 and 2018 could be a result of the 2018 implementation of the GDPR. Nevertheless, further full-text analysis of the articles showed that the rise of publications can not be attributed exclusively to the GDPR (see Section 4.4.5). Another interesting

[18] `https://eur-lex.europa.eu/eli/reg/2016/679/oj`, last accessed August 21, 2021

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

observation is the drop of publications in the year 2020, which could have several reasons. It is possible that in 2018 and 2019 the topic of privacy was considered more often due to the novelty of the GDPR, making those years the exceptions, as compared to 2017 the amount of publication is fairly steady. Another possible explanation is that in the first year of the COVID-19 pandemic, less publications about care robots were written, due to the novel uncertainty the situation brought. In Figure 3.3b it can also be seen that the approaches law and health science are not present – which could possibly also be attributed to the public health crisis of the COVID-19 pandemic, as scholars might have focused on related health and legal issues instead of writing about care robots. The number of publications from first authors of the academic discipline of health science dropped from 12 in 2019 to 4 in 2020. Throughout the whole year 2020 it also has been more difficult, if possible at all, to conduct empirical studies with care robots in residential care facilities, due to access limitations.



(a) Emphasizing the level of contribution (b) Emphasizing the approach to the topic

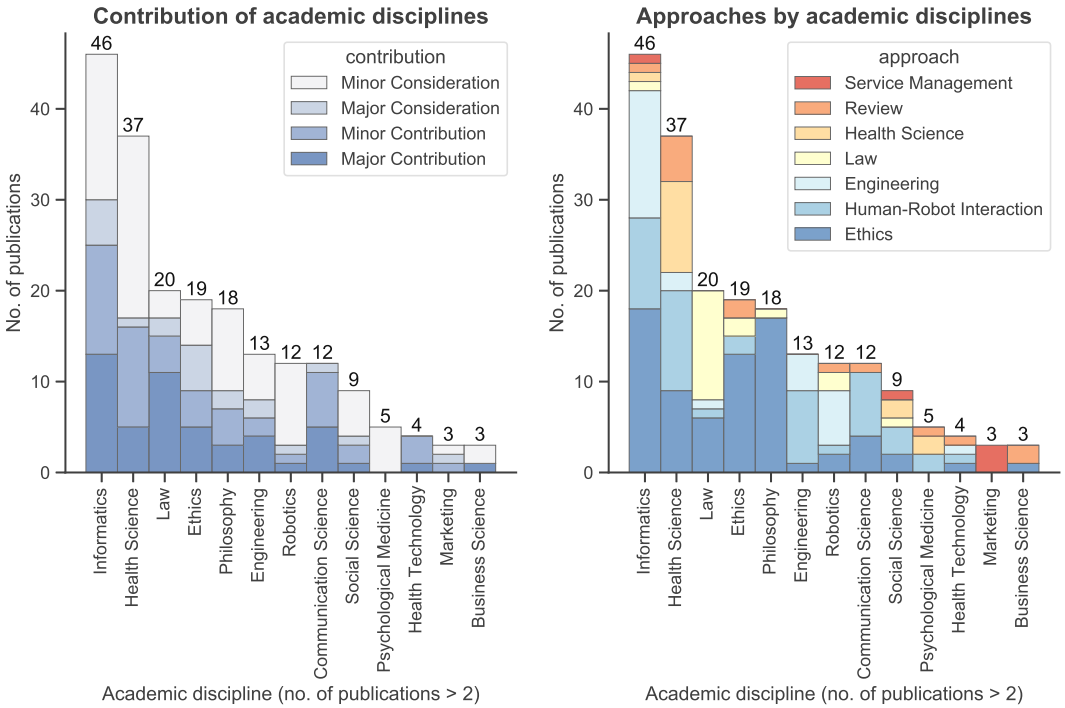
Figure 3.3: Number of publications per year (2010–2020)

Academic Disciplines

Figure 3.4 shows the different publications grouped by the academic disciplines of the first authors, as defined in the Tables A.1 to A.3. Only the disciplines are included, where at least 3 publications were identified in the screening. It is noteworthy that due to the interdisciplinary topic of robotics in combination with health care many of the analyzed publications were the result of multiple institutions from different academic disciplines working together. The results show that most (20.9%) of the first authors were publishing from a departments that fall under the category of informatics, such as computer science or software engineering etc., 16.8% of the records were published by authors from the health science disciplines. If considering the disciplines of philosophy (8.2%) and ethics (8.6%) together, they amount to 16.8%, thus this would be the second largest group of contributors to the discourse. Figure 3.4a also allows to analyze the level

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

of contribution of each academic discipline. In this regard it stands out that publications of the disciplines law, communication science and health technology tend to have a high proportion of minor or major contributions, while large parts of the disciplines health science, robotics and psychological medicine only include minor considerations of privacy aspects. In particular authors from the robotics discipline seemingly do not discuss the privacy aspects as much, and more focus on technical aspects of care robots. With regards to publications from the law discipline, the high amount of major contributions can be explained by considering that privacy due to it's nature as a human right is often seen through the lens of regulation but also violation of such right. Also in informatics privacy has a prominent role, with the focus lying on data protection and security in the digital sphere. Another interesting aspect is the general approach of the publications of each academic discipline, which can be seen in Figure 3.4b. While in informatics the approach is mostly split between engineering, human-robot interaction and ethics, in other disciplines the approach corresponds to the respective faculty or department. Authors from philosophy and ethics, approach their publications mainly by ethical considerations. The approach of human-robot interaction is most frequently taken by authors from the disciplines engineering and communication sciences. With regards to the disciplines of health science and law, it is also evident that those have the largest amount of health science respectively law approaches among the disciplines.



(a) Emphasizing the level of contribution (b) Emphasizing the approach to the topic

Figure 3.4: Number of publications per academic discipline

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Demographic Analysis

Figure 3.6 shows the number of publications per country of the institution that the first authors are affiliated with. Notably the number of publications from the United States, the United Kingdom and the Netherlands amount to nearly half of the overall records (45.0%), which could be in case of the first two mentioned be due to restricting to English-language publications in the database searches. The Netherlands stand out in this analysis as the EU country with most publishing authors with regards to privacy impact of care robots, followed by Italy and Germany. Other relevant publications with major contributions from Europe were published by Norwegian and Swiss institutions. In Asia and Oceania the most relevant literature is contributed by institutions from Australia and Japan. According to the classification of the United Nations (2019b), the vast majority of the countries listed in the results of the literature gathering belong to high-income countries; exceptions are China, Ecuador and Lebanon, which are classified as upper-middle-income countries, and solely Nigeria which belongs to the class of lower-middle-income countries. While this distribution of academic publications can for sure be attributed to the economic development of the different countries, it is as well a fairly good correlation in regards to the old-age dependency ratios of those nations. The projected percentage of the age group 65+ years by the United Nations (2019b) for high-income countries (2019: 18.0% – 2030: 22.0% – 2050: 26.9%), upper-middle-income countries (2019: 10.4% – 2030: 14.8% – 2050: 22.5%) and lower-middle-income countries (2019: 5.7% – 2030: 7.6% – 2050: 11.7%) respectively, suggests that researchers from countries from the first-mentioned group have more incentives to discuss the topic of care robots in regards to the care for the elderly in academics already, as the share of their old population was already higher in 2019 than it is projected for upper-middle-income countries by 2030 and for lower-middle-income countries by 2050.

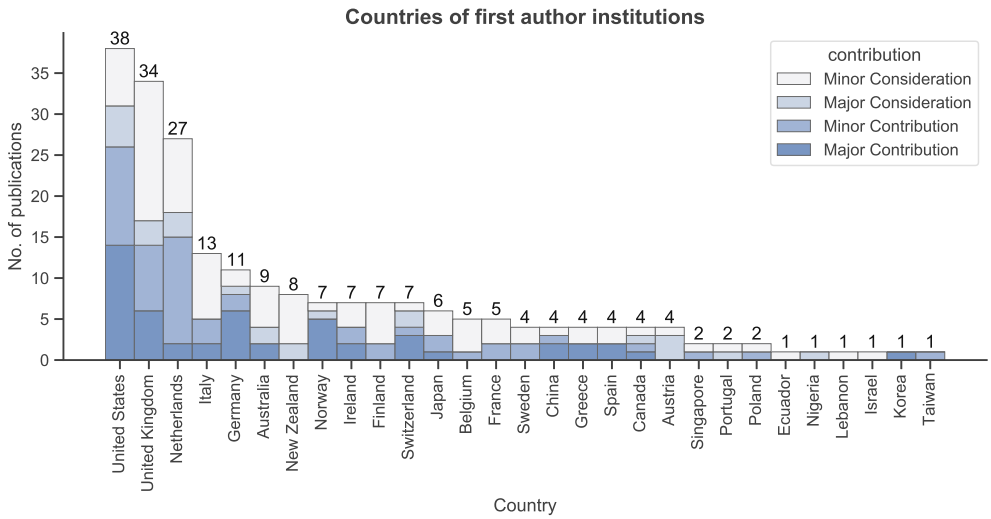


Figure 3.5: Publications by country of the institution of the first author

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

The first author field turned out to have high cardinality, meaning only a few authors have published on the topic more than once. Those first authors with two or more publications can be seen in Figure 3.6. Eduard Fosch-Villaronga (e.g., Eduard Fosch-Villaronga and Poulsen, 2021), currently affiliated with the Leiden University in the Netherlands contributed the most, with 7 overall publications and 3 major contributions. Apart from that, only Christoph Lutz from the BI Norwegian Business School (e.g., Lutz, Schöttler, et al., 2019) contributed more than three major publications to the topic (4 major contributions). Other top authors are Tijs Vandemeulebroucke (e.g., Vandemeulebroucke, Dzi, et al., 2021) from KU Leuven, Belgium, with 5 publications, Elizabeth Broadbent (e.g., Broadbent et al., 2018) affiliated with the University of Auckland, New Zealand with 4 and Mark Coeckelbergh (e.g., Coeckelbergh, 2016) from the De Montfort University, United Kingdom, who contributed 4 publications. Sharkey Amanda and Sharkey Noel (e.g., A. Sharkey and N. Sharkey, 2012), both of the University of Sheffield, United Kingdom, certainly can be considered as experts on the topic as well, as many of their publications were created in collaboration. It is worth noting that the affiliation of the authors with academic institutions changes over time, and thereby one author could be attributed to different countries in Figure 3.5.

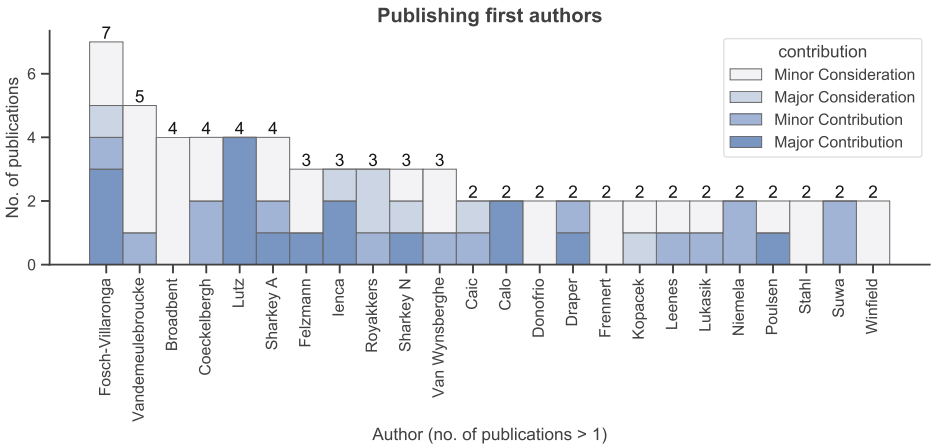


Figure 3.6: First authors with two or more publications

Figure 3.7 lists the institutions of the first authors at the time of the publication. Most records were written by authors from University of Twente in the Netherlands (8) and the University of Sheffield in the United Kingdom (8). It is also an interesting observation that authors from different academic disciplines from the same institutions were publishing on the topic.

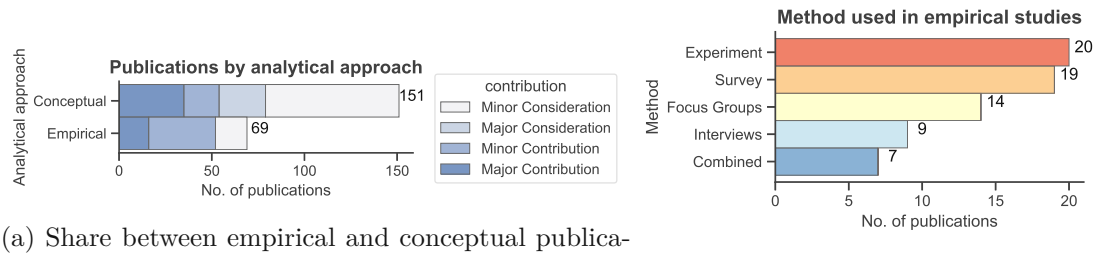
Analytical Approach

The screening included 151 (68.6%) conceptual works and 69 (31.4%) empirical works (see Figure 3.8a). Both analytical approaches add major contributions to the topic. In around half of the conceptual works, privacy is only considered in a minor way. It can be

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Figure 3.7: Publications by institutions of first authors (more than two publications)

seen that empirical studies are more likely to add at least a minor contribution to the discussion. The methods used in empirical studies can be seen in Figure 3.8b, mostly those studies are experiments or based on surveys.



(a) Share between empirical and conceptual publications

(b) Method used in empirical studies

Figure 3.8: Analytical approach and methods of empirical studies

Scholarly Publications

The following discusses the question of »where has been published?« There is a large variety among the scholarly publishers, Figure 3.9 therefore shows only the journals, conference proceedings or book chapters where three or more records included in literature review were published. The vast majority of the records (90.9%) was published in peer-reviewed publication outlets. There is a high number of records from the »International Journal on Social Robotics« (12) and the journal »Ethics and Information Technology« (9). Additionally it was attempted to attribute the main field of each publication outlet, which due to the interdisciplinary and multidisciplinary nature of those was not always clear. The results can be seen in Figure 3.10, the chart also includes the level of contributions from the different journal fields, and is limited to publishers where three or more publications have been found. The publishers which were categorized to be from

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

the fields »Informatics« and »Ethics« show a high number of major contributions.

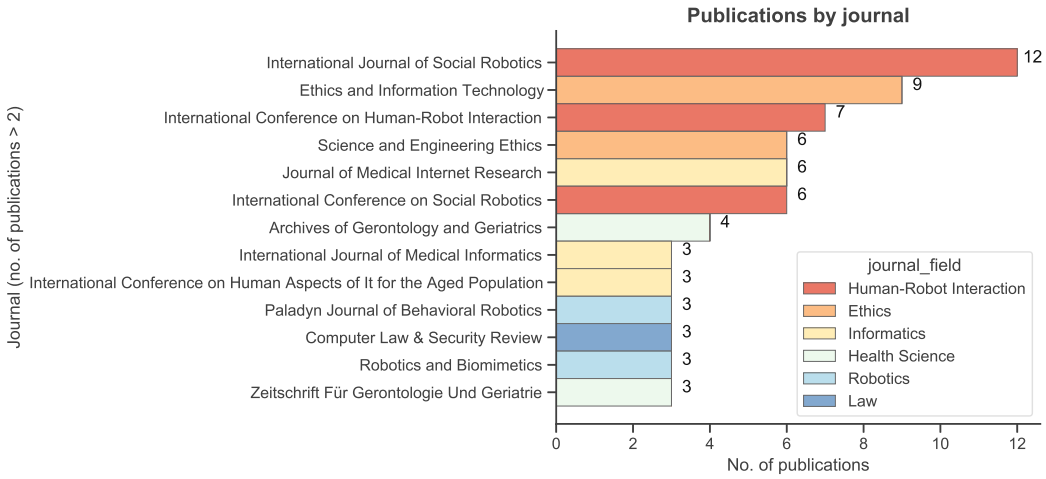


Figure 3.9: Publications by journals (more than 2 publications)

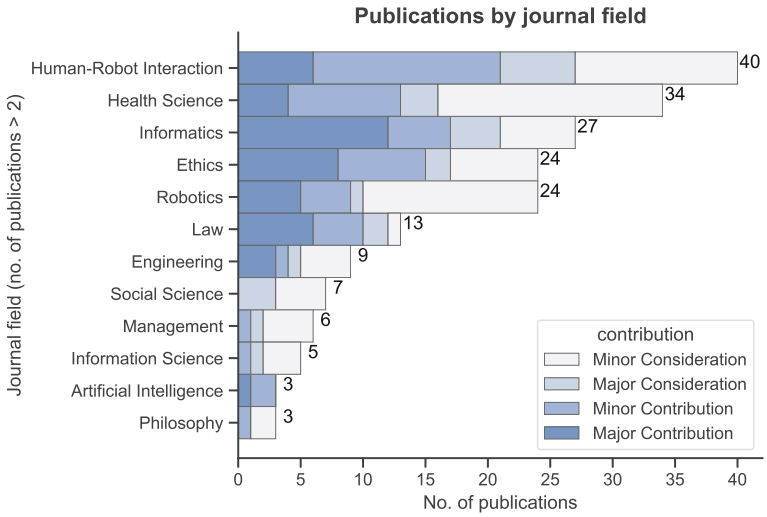


Figure 3.10: Publications by journal field (more than 2 publications)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

CHAPTER 4

Findings

In this chapter the contents of the publications identified in Chapter 3 are analyzed in detail to understand how privacy issues currently are being negotiated by the general scientific community. The discussion will relate to the defined technologies and concepts of privacy, as elaborated on in Chapter 2. The method used for the qualitative analysis is described in Section 3.2. Then the findings are discussed, in particular to give an answer to **RQb** ("How is privacy currently being negotiated in science?"). This chapter includes only the publications which were categorized as »major contributions« in the screening process (see method in Figure 3.1). The distribution of major contributions among the different academic disciplines can be seen in Figure 4.1. In the following chapters, the various aspects that arose during the analysis are addressed.

4.1 Dimensions of Privacy Discussed in Literature

In this work, privacy was considered in the four dimensions (i) physical, (ii) social, (iii) psychological, and (iv) informational, which is along the definition by Burgoon (1982). This multi-dimensional view reflects the facets of privacy in a very comprehensive, but also differentiated way. In the following, it will be elaborated which dimensions of privacy are addressed in the analyzed publications.

The publications by Rueben et al., Lutz, Schöttler, et al. (2019) and Reinhardt et al. (2021) also propose that these aforementioned four dimensions of privacy need to be accounted for when developing care robots. Alaiad and Zhou (2014) on the other hand, use a different four dimensional definition of privacy, which was proposed by Privacy International[15] – information privacy, bodily privacy, privacy of communications, and territorial privacy. Alaiad and Zhou state, that among those, informational privacy is the most relevant for the acceptance of robot technologies. In the Privacy International definition, the informational aspect is equivalent to Burgoon's definition, while the physical dimensions is split in bodily, so the protection of an intrusion to the body,

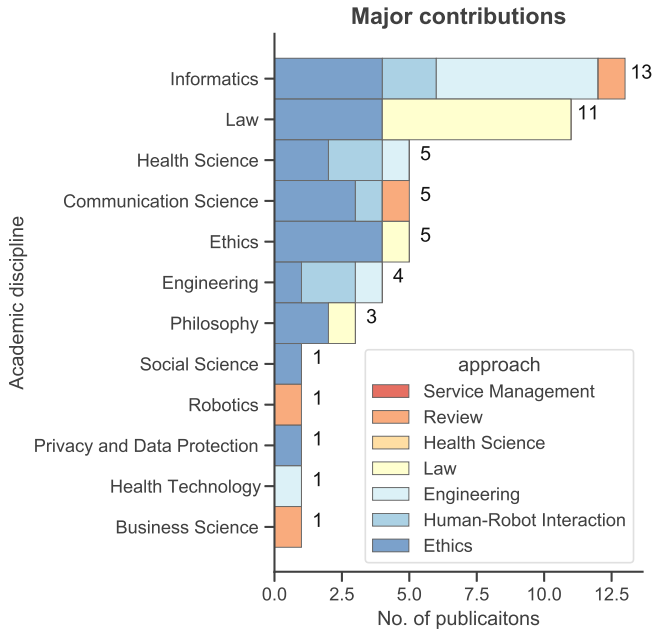


Figure 4.1: All major contributions by academic discipline

and territorial, e.g. an intrusion in the home. The privacy of communications on the other hand, includes both, the social and the psychological aspects which Burgoon was describing. Another variation of the privacy dimensions was used by Blake (2019), who considers three dimension of privacy: physical, informational and associational, whereas the latter is maintaining privacy of an individual towards family and friends – similar to social privacy. Armbrust et al. (2011) use the definition for privacy by Brandeis and Warren (1890) »the right of the individual to be let alone,« and thus aim to develop a care robot which minimizes the necessity of interference by caregivers, allowing maximum autonomy for the caretaker. This argumentation refers to the physical privacy of the robot's user – but it disregards that the robot itself can be perceived as an invasion to privacy. Also Yusif et al. (2016) distinguish between personal privacy, which they interpret along the view from Brandeis and Warren as the right to be left alone, and data privacy, so the right to control one's data. Those, again correlate to Burgoon's physical privacy and informational privacy. A view that also goes more towards the data processing aspect of privacy, is taken up by Ienca and Eduard Fosch-Villaronga (2019), who elaborate on different definitions of privacy, among them as the ability to control when, how and to what extend information about oneself is shared (Westin, 1968, as cited in Ienca and Eduard Fosch-Villaronga, 2019); they furthermore point out that privacy is a human right, as defined by the UDHR. A contrary view to the universal right to privacy is provided by Carnevale (2016), who argues that privacy is not an absolute right, but it depends on the context – as sometimes intrusion of privacy is warranted, interests must be balanced –, and the particular domain, where different standards for privacy

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

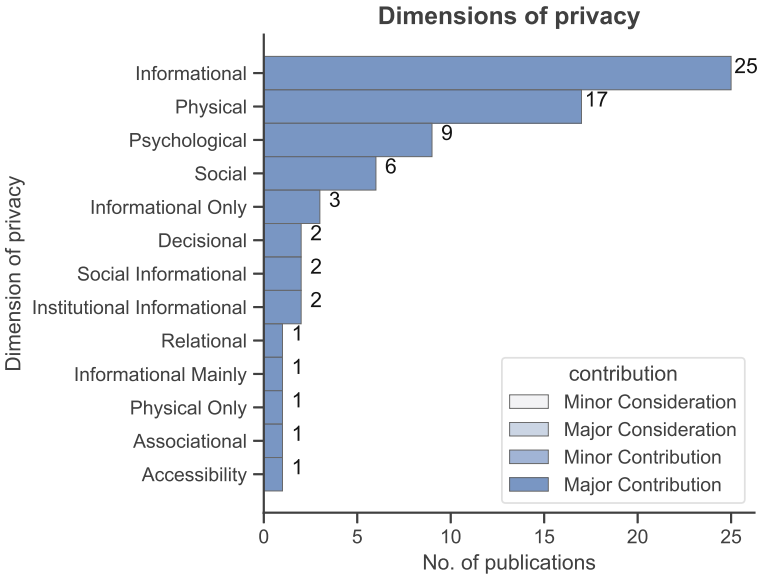


Figure 4.2: Dimensions of privacy discussed in literature

violations could exist. A. Sharkey and N. Sharkey (2012) on the other hand emphasize that privacy is a human right as well as a human value, which has to be protected.

4.1.1 A Focus on Informational Privacy

As it can be seen in Figure 4.2, the literature review identified a large proportion of publications that discuss the informational aspect of privacy – some also explicitly only focus on the informational aspects, disregarding other dimensions (e.g., Bartoletti, 2019; Felzmann et al., 2016; Vallverdú and Casacuberta, 2015). This is partly justified from the point of view of data processing, data storage, data collection using machine learning algorithms, and also by legislation that focuses strongly on these data protection aspects, such as the GDPR. Lutz, Schöttler, et al. (2019) found in their scoping literature review to assess the privacy implications of social robots, that many publications mostly analyze the aspects related to informational privacy, and if no particular definition of privacy is included in the respective study, informational privacy was the implied concept. At the same time, Lutz, Schöttler, et al. are highlighting that privacy implications of social robots go way beyond of the implications of established technology due to their mobility, and social meaning of robots – the latter they found to be the most important characteristic. Sedenberg et al. (2016) also focus on informational privacy in their study, and only touch on psychological privacy. This imbalanced focus on informational privacy, however, does not reflect the sentiments of users of robots; for example Schomakers and Ziefle (2019) found in their study, that respondents do not only care about informational privacy, as also obtrusiveness of the technology in the home was perceived as important. In another empirical study that García-Soler et al. (2018) conducted with focus groups with overall

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

67 participants, privacy concerns linked to the dimensions of informational and physical privacy were found. García-Soler et al. formulated requirements for the inclusion of care robots into the life of elderly users from the results of the focus groups, where an important requirement was that only authorized personnel should be granted access to the robot, which implies the (i) prevention of unauthorized persons to gather personal information about the client, and (ii) the prevention of a physical intrusion to the home of the user. Another requirement García-Soler et al. formulated which is linked to both physical and informational privacy is the prevention of malignant uses by designing a secure system, which could be related to physical harm, or harm by unwanted data dissemination. The requirements of safe storage and collection of personal information formulated by García-Soler et al., clearly are linked primarily to informational privacy, while on and off features could relate to both, preventing a physical invasion or stopping e.g. recording of personal data. The requirements that García-Soler et al. formulated, also are in line with the aspects of having control over one's own data, as Burgoon (1982) described in the part on informational privacy.

It was found that in empirical studies mainly the aspects of physical and informational privacy are taken into account, in any case, it is quite obvious that it would be wrong to consider only the informational aspects, since users value physical safety highly. The insight gained from the literature review is that the dimension of informational privacy is the most discussed in current literature, followed by the physical privacy aspect.

A contrary conclusion to this literature review and also the scoping literature review on the privacy implications of social robots by Lutz, Schöttler, et al. (2019), which states a predominant share of publications on informational privacy, was drawn by Ienca, Wangmo, et al. (2018). In a descriptive review with n=571 articles, Ienca, Wangmo, et al. found that non-invasiveness, non-intrusiveness and non-obtrusiveness were discussed –relating to physical privacy –, while privacy tracking and monitoring were the main topics regarding informational privacy; and they state that proactive security and data protection are only considered in one of the Intelligent Assistive Technologies (IATs) that were analyzed and thus, they are in favor of a more frequent consideration of informational privacy aspects.

4.2 Notions on the Privacy Impact of Care Robots

In this section the general notions on the privacy impact of care robots are discussed, as it was found while reviewing the literature that the attitudes, both of researchers and subjects in empirical studies, vary significantly. As shown in Section 3.3, there is a large amount of publications on the topic of care robots, that do not consider much whether the robot they develop has much impact on privacy. The following sections will summarize the predominant notions.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

4.2.1 User Perceptions

While Lutz, Schöttler, et al. (2019) have stated that there is a lack of survey based evidence, the following examples may help to gain an overview of the privacy attitudes of users towards care robots. Lutz and Tamó-Larrieux (2020) conducted a survey with 480 participants on the attitudes towards privacy with robots. In the survey, Lutz and Tamó-Larrieux distinguish between three types of privacy concerns in their survey: (i) physical, related to the intrusiveness of robots, (ii) institutional privacy, which is about the way data is processed by e.g. robot manufacturers, governments or third parties, and (iii) social informational privacy which is concerned about data processed by individuals such as family but also hackers. Lutz and Tamó-Larrieux found in their survey, that respondents are most concerned with the data protection by the companies that supply the robots (i.e., the institutional privacy aspects), and they are somewhat concerned about hackers which would use robots for malicious practices (i.e., social informational privacy), while they seem not to be concerned about physical privacy. Overall, Lutz and Tamó-Larrieux found that there is only moderate concerns related to privacy impact of social robots, and that the perceived benefits had a positive effect on the attitudes towards social robots. Moreover, Lutz and Tamó-Larrieux point out that the privacy concerns should be taken into account by robot manufacturers when designing robots.

Yusif et al. (2016) found in a systematic review about the willingness of adoption of assistive technologies, that privacy is a top concern for older adults, with 34% of the 44 articles examined naming it. Another survey with 1090 older adults by Reinhardt et al. (2021) discovered that female respondents were more concerned about their privacy. Draper and Sorell (2017) limit their definition of privacy to a state where there is restricted access to information about an individual, which also included the information that can be gathered by observation. In an experiment with focus groups, Draper and Sorell found that robots can pose an unwelcome intrusion into privacy, while there was less reservations and even some support if the observers were healthcare personnel, as the robot then perceived as merely a medical tool – presumably applying the norms of medical confidentiality. Moreover, Draper and Sorell found that participants were more concerned if health information would be shared with relatives or other informal caretakers, than with healthcare personnel. These two observations are in some way opposite to the finding by Burgoon (1982), whereas an individual would perceive an intrusion into the home by relatives less of a violation to privacy than an intrusion by a stranger that can not be regarded a nonperson. Although this finding is relating to the physical dimension of privacy instead of informational privacy as this example constitutes, it seems contradictory that an individual would be more concerned about relatives having access to health data, than they would hesitations to have a stranger – what a professional carer nonetheless is – access it. Apparently the mentioned medical confidentiality by Draper and Sorell is a powerful way to mitigate privacy concerns, as it forms a contract based on trust with the individual and clarifies the questions of »who has access« and »why does the person have access.«

Eduard Fosch-Villaronga, Tamò-Larrieux, et al. (2018) did a workshop on ethical, legal

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

and societal (ELS) implications of social robots, where they identified security and privacy as a key challenges. The participants of the workshop elaborated to what unprecedented degree robots affect privacy: they move around, they can capture videos monitor the environment with sensors, interact with individuals and record those interactions, and furthermore collect data about daily routines of the users around.

D. Yang et al. (2021) found that users are especially sensitive regarding privacy if nakedness is involved, a fact that was also observed by Fernandes et al. (2016). Fernandes et al. found in a survey with 449 participants that about 78% consider privacy at home very important, with around a third of the respondents saying they are most concerned about nakedness. While turning off the camera would also be a feasible solution to avoid recording nakedness and such, the authors found that the preferred option is a robot detecting a situation and turning away completely, as for robot that would only stop recording there is no way to control it – it is this simple psychological effect that according to Fernandes et al. makes the difference of how people perceive their privacy loss. Finally they conclude that while 74% agreed that the turning away is the best option for privacy-sensitive situations, 28% of the respondents still feel uncomfortable about the robot staying in the same room. In a survey (n=104) Alaiad and Zhou (2014) confirmed their hypotheses, that privacy concerns have a negative effect on the intention to use home healthcare robots (HHRs) and also on trust. Wu et al. (2021) found in their study that even the unintended exposure of certain areas of the home was perceived as privacy infringement. Draper and Sorell (2017) found in an experiment with focus groups that participants have different perceptions of whether monitoring is a privacy violation, depending on the reason for recording, the means of recording, the subject of the recording, who has access and on whose authority. Hoorn et al. (2015) found that care robots can even help by providing privacy when assisting in intimate moments – as older people are sometimes ashamed of their body, they prefer not to be exposed to a human caretaker. They also found that there was no concern about whether information would be disclosed, unless the elder ladies participating in the experiment were repeatedly told that they should be concerned.

In an empirical study that García-Soler et al. (2018) conducted with focus groups with overall 67 participants, requirements for the inclusion of care robots into the life of elderly users were formulated. Regarding privacy they were able to identify the following requirements:

1. Only authorized persons should be able to access the remote operator
2. An authentication procedure should be required
3. Robust security system should be developed to avoid malignant uses
4. The user should be informed if the remote operator changes
5. The user should be able to override the remote control
6. Storage of personal information storage should be in safe databases
7. Collection of information should be restricted to useful information

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

8. The system should have a customizable and accessible on/off system suited to the specific user needs

(García-Soler et al., 2018, p.194)

Apart from these requirements for privacy especially, García-Soler et al. (2018) formulated requirements regarding safety and privacy, namely that robots should announce actions to be taken and communicate them in real time. Those requirements show in condensed form the notions about privacy impacts of care robots, whereas the control over the data and the robot, authentication, as well as the security of the storage shall be pointed out. Also it can be seen, that the requirements include mostly aspects related to informational privacy, and some to physical privacy, while social and psychological privacy are not addressed.

4.2.2 Researcher Perceptions

Armbrust et al. (2011) project, that concerns about privacy might lead to an unfavourably low acceptance of robots in care. Similarly to this opinion, Heuer, Schiering, and Reinhard Gerndt (2017) point out that awareness for the privacy risks of robots is important for users, and thus for the acceptance of the technology, which calls for transparency and a thorough consideration of privacy issues linked with the functionalities of the robot. Furthermore, Heuer, Schiering, and Reinhard Gerndt find clear words about the future dangers that robots bring with them and call for these aspects to be considered already during development:

> Robots will be dangerously ubiquitous, but, as for other smart devices as e.g. smart phones, wearables, etc. that accompany users in their daily life, the privacy risks are not obvious. Hence, privacy should be an important aspect in robotics, but is not taken into consideration in a satisfactory way yet. At the moment robots are designed from an engineering perspective with a main focus on functionality. Privacy and other ethical aspects of robotics are investigated in general, but not adequately integrated in the engineering process of robotics (Heuer, Schiering, and Reinhard Gerndt, 2017, p.266)

Ienca, Wangmo, et al. (2018) point out that designers of IATs should be proactive rather than reactive regarding value-sensitive design, including privacy aspects, of the technology. Also, the fact that privacy plays a minor role in the development of assistance systems is something that has been noted: Ienca, Wangmo, et al. performed a descriptive review with n=571 articles, analyzing the ethical considerations in publications on IAT technologies for people with dementia, finding that the majority of them are designed in absence of ethical considerations. Furthermore, they found that in the publications which list ethical aspects, merely 5% considered privacy – the smallest portion among the other ethical considerations. Lutz, Schöttler, et al. (2019) conclude that the body of empirical knowledge on the topic of privacy implications of social robots is thin and the sample sizes are small, with non representative results, and that those studies available mostly focus on informational privacy aspects. Furthermore, experts that

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Lutz, Schöttler, et al. interviewed, call for interdisciplinary discussions on the topic. Calo (2020) concludes that that neither law nor technology has prevent privacy harm effectively, and thus development of social robots should be proceeded carefully. An interesting aspect regarding consideration of privacy aspects in the design of robotic care technologies, is discussed by Lutz and Tamò (2015) which find a conflict of efficiency and effectivity: in the »engineer's rationality« the question is whether something is done how it is supposed to, and that engineers often do not see it as their responsibility to implement privacy considerations into their designs, but rather focus on the outcomes in terms of functionality. In contrast to that, Lutz and Tamò argue effectivitiy describes whether the right things are done, and they point out that the regulators responsibility is the empowerment of consumers. Ienca and Eduard Fosch-Villaronga (2019) differentiate privacy and data protection – data protection just focuses on the processing of personal data, while privacy ranges in multiple dimensions in the private life of a person; they argue that privacy thus has a broader range, on the other hand under data protection there also falls data that is not a concern to an individual's privacy.

Novitzky et al. (2015) performed a systematic literature review, with an included initial 350 sources, especially focusing on ethical aspects of AAL technologies in relation to people with dementia. They summarize their findings, saying that concerns about safety, security and privacy are focused on the most, when discussing ethical challenges. Rueben et al. (2018) discuss several seven themes that will be important for understanding the privacy impact of robots: (1) data storage, (2) manipulation, (3) trust, (4) blame, (5) privacy regulation, (6) special private domains, and (7) privacy scholarship outside human-robot interaction (HRI). Kaminski (2014) finds that robots in the home, might cause two types of privacy infringement: (i) challenges to boundary management and (ii) the violation of contextual integrity. Lutz and Tamò (2016) find that social robots affect privacy in the four overlapping dimensions informational, social, psychological and physical privacy, and analyze the privacy impact of care robots using the Actor Network Theory (ANT) which takes the agency of objects as well as the social and technological relationality into account. Schulz et al. (2018) use Palen and Dourish's framework (Palen and Dourish, 2003) to assess the different boundaries along which privacy is negotiated in an robotic care setting. They point out that compared to AAL systems, which have stationary cameras, robots might be better for elderly patients to relate to and understand their sensory capabilities – and thus, understand the privacy issues involved. In regards to AAL technologies, Novitzky et al. (2015) point out that indispensable third parties that have no direct health responsibilities, e.g. providers of electricity and internet connections, could have responsibilities and also might infringe privacy and confidentiality.

Theoharidou et al. (2017) assessed the requirements for health care in a smart home context, finding the main groups to be anonymity and unlinkability, the compliance with policy and law, the patient's ability to have control over data (which includes also informed consent) and measures regarding security. Theoharidou et al. also point out that smart home healthcare devices range from simple devices to intelligent devices,

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

which come with different challenges for privacy. The authors calls for best a practice guide regarding privacy in health care smart homes, which should also take into account emerging technologies such as cloud technology and the internet of things. Vallverdú and Casacuberta (2015) are discussing privacy in the context of medical machines which they identify as one of the main ethical problems, and point out the problem of health data and big data processing, where they find that it is unlikely that a person would accept a third-party database to store personal information about oneself. Eduard Fosch-Villaronga and Roig (2017) argue that since robots are capable of recording everything in their environment they could pose major challenges for data protection concerning the awareness of the data collected, informed consent and legitimate purpose for the data collection. Eduard Fosch-Villaronga and Albo-Canals (2019) discuss in their study the ethical and legal aspects of robots used in therapy – meaning both physical and cognitive rehabilitation therapy –, that affect multiple dimensions of privacy: (i) due to the anthropomorphic design, the user might not recognize the capabilities of surveillance that the device has, compared to a device explicitly designed for surveillance, (ii) it has shown effective for therapy that the devices show emotions, which encourages users to also show emotions openly which can be recorded, (iii) the cyber-physical nature of social robots complicates security and thus threatens privacy, as physical as well as digital security has to be ensured, with the complexity increasing as new technologies such as cloud computing and blockchain are used.

In their paper, Lutz and Tamò (2015) discuss mainly the impacts of care robots on informational privacy (control of information that allows personal identification) along the three dimensions described by Calo (2020): privacy infringements by (i) surveillance, (ii) access to sensitive personal information, and (iii) social meaning; while they point out that those can those may overlap or even reinforce each other. Blake (2019) conclude that care robots threaten privacy, confidentiality and autonomy, which could influence the trust of patients into medicine. A. Sharkey and N. Sharkey (2012) raise their concerns more general, asking if the right to privacy is infringed by being monitored – regardless of whether access to the video was obtained in a malicious way, or by relatives respectively caretakers. Cognitive impaired people on the other hand A. Sharkey and N. Sharkey argue, may even forget that a monitoring device was in the room which creates a wrong sense of privacy. According to A. Sharkey and N. Sharkey there is often a lack of protection for the human rights of the elderly, and there is no protection of the potential downsides of robots in care. Calo (2011) argues that social robots will interfere with one's right to be let alone. Caine et al. (2012) expect that older adults will engage in privacy enhancing behaviors (PEBs), among various other unexpected behaviors, when they are concerned about their privacy due to monitoring at home. Bartoletti (2019) points out another challenge, which is that privacy is culturally bound, evolves over time and influenced by cultural norms – thus it is likely that it will also evolve along technological development. Frik et al. (2019) dive into the different understanding of privacy that older people have: some see it as a valuable human right, that needs protection, others say that older people do not have to worry as much about privacy as younger people, as their data is not as valuable for profiteers. Jecker (2020) states that the meaning of »private« could

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

change, as the understanding of what information is considered private changes, which could lead to people being less reserved and have also more social relationships. What could depersonalize relationships with robots, is according to Jecker if the producers of the robot, which are for-profit companies, force the user to listen to advertisements on the robot before an interaction – similar to free-to-use services such as YouTube. Thus, according to Jecker it matters to protect privacy in human-robot relationships, as it might help to create a real relationship, that is not based on a for-profit company making money from the users' information or data.

Novitzky et al. (2015) found that enabling patients to age at home can have positive effects for privacy, personal integrity, dignity and the self-image, as the alternative is being institutionalized with other co-habitants. On the other hand, they found that too much hospital technology at home could disrupt the special meaning of a home as a place of confidence, trust, safety and privacy. The main benefits of IATs for patients with dementia found in literature, Ienca and Eduard Fosch-Villaronga (2019) point out, are (i) increased autonomy, and the possibility to age at home; (ii) a better, healthier lifestyle with preserved functional capabilities; (iii) reducing social isolation; (iv) supporting professional and informal caretakers; and (v) a more efficient use of resources in an aging society.

4.2.3 Conflicting Values

The advantages and disadvantages of care robots are also discussed in the literature on the basis of conflicts that the technology brings with it. These are often discussed in the reviewed publications, but the resolution of the conflicts is usually not given - as these depend on the individual values of the users.

Privacy vs. Safety

Huber and Camp (2017) found that privacy concerns are not the major consideration of elderly people, but the maintenance of key relationships, they quote one an 80 year old participant of their experiment stating: »If it helps my son to feel better about taking care of me, I don't care what he wants to install« (p.96). Van Heek et al. (2017) researched the acceptance of AAL systems. They came to the conclusion that there is a trade-off between the benefits that users of such technologies experience, which are especially autonomy and safety, and privacy concerns. The more the users are depending on such a system, e.g. if they are older, disabled or needing other care, the attitudes towards privacy are influenced significantly, meaning that those groups show higher intentions to use AAL technologies (Van Heek et al., 2017). Related to the conflicting values of safety and privacy, N. Sharkey and A. Sharkey (2011) discuss whether robots should be allowed to intervene in cases of irresponsible behavior of a patient, e.g. should a robot prevent an elderly person to drink alcohol. Taking such fundamental liberty rights without a due process, N. Sharkey and A. Sharkey argue, could result in what they call »authoritarian robotics.« N. Sharkey and A. Sharkey continue that the duty of a carer is to take care of the patients safety, but not with all means, as patients have

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

the right for personal liberty, the right to be protected from psychological harm and the right to privacy. N. Sharkey and A. Sharkey find that the trade-off must be individual for each patient, e.g. a patient should have the liberty to open a drawer with kitchen knives, but if the patient has suicidal tendencies such behavior should be avoided; another conflict with privacy would be if a patient is in intensive care, 24 hour monitoring would be appropriate, but not in other cases – a care robot should be able to understand the context and behave accordingly. N. Sharkey and A. Sharkey find that it is paradoxical that the more safety a robot can provide, the more their usage might actually break human rights. They also find that the violation of privacy would be perceived in other ways for different target groups, and argue that for example children would have less of a problem with being filmed on a toilet than an elderly person, assuming that the images are not recorded and can in the case of the children just be watched by their parents. Thorstensen (2018) investigates the privacy impact of AAL technologies and how automated decisions regarding health made by the system could be in conflict with the GDPR, which demands consent in such situations – which potentially could be a conflict of health and privacy, as useful health measures could be omitted for privacy. Schafer and Edwards (2017) point that while it would be better in terms of privacy that sensory capabilities are transparent, e.g. that the sensors are visible for users, at the same time visible sensors on a self-driving could be targeted by vandals and cause a safety problem if they are malfunctioning after an attack.

Ienca and Eduard Fosch-Villaronga (2019) identify the conflict between preserving the patients safety and well-being by providing the maximum possible quality of care, and the possible privacy infringements:

> [...] renouncing to the implementation of monitoring and tracking technology altogether on the grounds of privacy rights would dramatically hamper the quality of care, obstacle improvements to the quality of life of the patient and delay technological innovation. At the same time, however, allowing the unrestricted collection and dissemination of personal information (e.g. behavioral or physiological) from elders with dementia without their knowledge and consent, could result in disproportionately invading the private sphere of these patients and ultimately producing injustice. (Ienca and Eduard Fosch-Villaronga, 2019, p.5)

Privacy vs. Perceived Benefits

Lutz and Tamó-Larrieux (2020) found that the perceived benefits had a positive effect on the attitudes towards social robots. Townsend et al. (2011) point out that older adults are willing to trade privacy, if they can gain autonomy – finding that even cameras were acceptable, depending on the amount of autonomy created by the monitoring technology. Frik et al. (2019) found that patients would be willing to treat a degree of surveillance, e.g. relatives monitoring them for safety concerns, for more autonomy while at home. Schomakers and Ziefle (2019) point out that the usefulness of a AAL system might exceed the privacy concerns – which should be taken into account to understand user choices. In contrast to the reserved opinions in favor of preserving privacy, Ienca, Wangmo, et al. (2018) point out that there needs to be a balance between privacy concerns and the

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

benefits of the IATs, as e.g. minimizing invasiveness or obstruiveness may lead to less accurate sensing and tracking results, which could negatively impact the health benefits of the technology. In other words, privacy needs to be balanced with principle of beneficence, meaning that every decision made should be for the best interest of the patient's welfare (Ienca and Eduard Fosch-Villaronga, 2019). Lutz and Tamò (2015) argue that it is valuable to develop care robots, as long as the developed technology would outweigh the values rather than the disvalues. This view is shared by, N. Sharkey and A. Sharkey (2011) which point out that the advantages of care robots are overwhelming, enabling patients to stay at home longer, thus increasing their independence. N. Sharkey and A. Sharkey argue also against replacing human care takers, as they can deliver important human contact, which can prevent loneliness – but also point out that there are some robotic solutions that can even be helpful for gaining companionship, e.g. robot pets that might even lead to a feeling of control and autonomy with patients. Despite various ethical concerns, A. Sharkey and N. Sharkey find that robot technology can contribute positively to the physical and mental welfare of the elderly, when it is used in appropriate ways; and thus, they argue that precautions have to be taken when proceeding with the development of such technologies.

A detrimental effect that care robotic technology could also bring is dependence on the technology. Novitzky et al. (2015) find that patients might become dependent on AAL technologies, to a degree that their autonomy is reduced. As an example they name that an over-dependent user might wait for the system to report an incident, instead of taking the matter in their own hands. Novitzky et al. state that this over-dependence could also drastically reduce the validity of informed consent given.

4.3 Privacy Concerns Caused by Care Robots

Figure 4.3 shows the concerns by care robots which were identified in the analyzed body of literature. The concern that is most frequently described is that of surveillance. This is discussed in different variants: (i) surveillance by unauthorized individuals or organizations, or (ii) surveillance by entities that have legal access, such as governments with a respective resolution. Other aspects relate to accessing sensitive data (access), taking control of the robotic device in a private space, and apprehensions about emerging technologies. The various concerns are grouped and described in the following sections.

4.3.1 Surveillance, Monitoring and Spying

The most obvious threat to privacy by robotics it the possibility of direct surveillance – unauthorized as by private parties or lawful as by governments (Calo, 2011, 2020). Calo (2011) warns in detail about the growing possibilities that are emerging with robotic technologies and AI in regards to surveillance and access: governments could get access to sensory information, such as audio and video, lawfully, and not only could they as such spy on a person but the could move the robot and thus the camera to actively search the home. While such an intrusion to physical privacy – into the home – seems unreasonable,

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

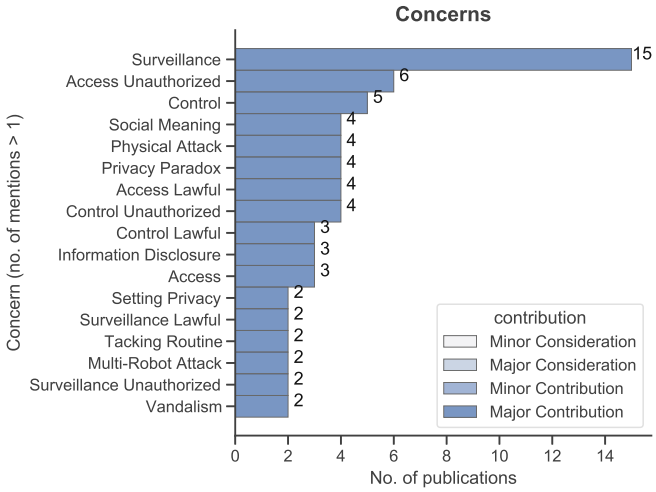


Figure 4.3: Discussed concerns posed by care robots

Calo (2011) argues that it would be acceptable even by the definition of the ECHR (Article 8), as the interference would be »in accordance with the law.« Alaiad and Zhou (2014) point out the usage of home healthcare robots (HHRs) could lead to tracking of the physical location; they point out that collection of data is especially of concern if the data is available to third parties. The threat of surveillance is also acknowledged by Demiris et al. (2009), which propose shape extraction to create anonymity for those observed (see Section 4.4.6). Unauthorized surveillance can be achieved far to easy with current robotic systems, as Denning et al. (2009) point out in an experiment. They authors exploited the security issues of Rovio, a mobile webcam robot, which also is used in eldercare, to supervise or virtually visit people that receive care for example by their by relatives. Denning et al. find that the video stream of the robot can be intercepted, which allows spying on people and furthermore, if the login credentials are acquired, the robot could be controlled by an attacker and even cause harm to care receivers, such as provoking them to trip. Spying or surveillance, is both, a violation to physical privacy by intrusion into the home sphere, as well as to informational privacy as the video data could be used to create information – such as routines, location and personal information stored inside the home. Frik et al. (2019) conducted semi-structured interview with 46 older adults regarding privacy and security threats they face with emerging technologies. Along those lines, Frik et al. explored the concern of surveillance, which they on the one hand discuss on the aspect of personal stalking, government or political surveillance, but on the other hand the surveillance by family members or medical staff in a care setting. While the intentions for such »care surveillance« are not bad, i.e. relating to safety concerns or monitoring of health data, Frik et al. find that such surveillance still causes stress, anxiety and annoyance and privacy concerns among their study participants. In regards to that, Frik et al. found that the poorly defined legal role of informal caregivers, such as family members and relatives, is what causes said annoyances, and concerns

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

about privacy and security. Frik et al. warn about the possible conflict of treating a degree of surveillance for more autonomy. Furthermore, surveillance is brought up in regards to assisted living facilities and nursing homes, where elderly move as a result of deteriorating health condition, and thus they are more resigned about »giving up privacy in exchange for safety and care« (Frik et al., 2019). Nevertheless, Draper and Sorell (2017) found in an experiment with focus groups that participants have different perceptions of whether monitoring is a privacy violation, depending on the reason for recording, the means of recording, the subject of the recording, who has access and on whose authority. Moreover Draper and Sorell found that the security standards and the storage duration on the data-storage is a decisive factor. Schomakers and Ziefle (2019) conducted a study on the privacy perceptions with AAL technologies where they found that misuse of data is the most pressing privacy concern, but also feeling surveilled and obtrusive technology.

Niemelä et al. (2017) found that the privacy aspect is not only important for patients, but for family members as well. In a study they found that residents sometimes did not notice that a video connection was opened, creating a feeling of spying with the calling family member. Despite that, the family member stated that they would agree to surveillance, if the resident would suffer from dementia, but also only with pre-acceptance of the resident (Niemelä et al., 2017).

One thing to consider, anyway, is the finding of Caine et al. (2012), that older adults will engage in privacy enhancing behaviors (PEBs) when they are concerned about their privacy due to monitoring at home. The study of Caine et al. considered different forms of monitoring and how it affects PEBs; they then implemented those in their experimental setup: a camera, a stationary robot with camera, and a mobile robot with a camera; finding that older people engage in less PEBs around robots – the possible explanation to that is that the participants of the experiment were not aware that they are being actually monitored, but only that there is the possibility they could be monitored. Caine et al. interpret this as an example of the various unexpected behaviors people engage in to protect their privacy.

4.3.2 Intrusion, Access and Control

Social robots or telepresence robots brings according to Ienca and Eduard Fosch-Villaronga (2019) not only challenges for data collection but to the invasion of the private life – in fact they point out that such robots could even cause physical harm; moreover they find that agreements and contracts made through telepresence robots, need to unambiguous and clear to avoid any abuse. Also, Li and T. Zhang (2017) find that illegal access and control with malicious intent can also cause physical harm; Denning et al. (2009) even showed in an experiment, that if the login credentials are acquired, the robot could be controlled by an attacker and even cause harm to care receivers, such as provoking them to trip. Using the robot to cause an accident adds more to the harm of physical privacy, by means of invading the bodily sphere and even threatening the safety and well-being of the individual. Eduard Fosch-Villaronga and Roig (2017) therefore point out that the

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

invasion of human space in shared environments is important, to research acceptance of social robot technologies in HRI. Calo (2020) argues that privacy is threatened by allowing the access to protected spaces, presenting information of the interior living space to hackers or governments, and also due to the social meaning of robots, the potential reveal of sensitive personal information from analyzing settings and usage statistics (»setting privacy«).

Frik et al. (2019) found that the participants of their study were are aware that loss of data, location tracking etc. can lead to physical attacks on them or their property. Another aspect the study by Frik et al. brought up is the privacy as bystanders, meaning if technologies are in the same room and the users might not even be aware of it – the use of such by others causing uncomfortable feelings to the bystanders. This phenomenon was also discovered in the study by Lutz and Tamò (2016) using Actor Network Theory (ANT): a robot does not only impact the patient, but occasionally also bystanders – creating a conflict as the bystander might not have consented to the robot recording information about them.

4.3.3 Social Meaning

Calo (2020) find that the unique social meaning, that social robots are attributed due to their sometimes anthropomorphic and socially interactive design, is impacting privacy. Heuer, Schiering, and Reinhard Gerndt (2017) find that the potential emotional bond and the attachment to robots is currently not seen as a major problem, while also pointing out that with a robot companion that is designed friendly looking there is potentially a higher willingness to blindly trust and share personal information with them. The emotional bond and sharing of personal, maybe even intimate information, is closely linked to the dimension of social and psychological privacy as defined by Burgoon (1982) – thus, when social robots trigger those feelings, there might be a potential privacy issue occurring. Lutz, Schöttler, et al. (2019) conducted a scoping literature review to assess the privacy implications of social robots and they found social meaning to be the most important characteristic. Calo (2020) voiced concerns that social technology could be used to elicit confident information (robot interrogators), and adds that in general the law is not well prepared to deal with the social dimension of robots and the harm it can cause, as »notice and and consent tend to defeat privacy claims« (p.24). These concerns are also shared by Frik et al. (2019), who elaborate on the fears that older people have regarding social-engineering attacks, as they believe that they are viewed as more vulnerable easy targets with lower technical awareness. Moreover, Frik et al. found in semi-structured interviews with older adults, that some participants fear to be influenced in their decisions, and they mention as an example the interference by social media into the US elections of 2016. This example shows that older adults are well aware of the possibility to be influenced in their values and opinions by technology; and it is illustrative for an impact on psychological privacy.

Jecker (2020) discusses using social robots to fill the gaps of human social contact during pandemic outbreaks, such as the COVID-19 pandemic, arguing that isolation

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

and loneliness pose serious threats to the health and well-being of older adults. Jecker elaborates on the challenges that social robots bring: (i) a higher probability of disclosing secrets or other intimate information as compared to other types of robots, (ii) the necessity to share private information in order for a relationship to develop and (iii) in a human-robot relationship, the human bears the greater risk as the robots record images, audio and data about them which could be accessed by others. In response to those challenges, Jecker point out that privacy should be put in the context of digital information sharing and thus, the risk that people already take when they share data on social media, with voice assistants, online banking and such; according to Jecker it is unclear whether social robots pose a greater risk, or create new risks. Lutz and Tamò (2016) also find that the social privacy aspect should not be neglected in care robotics, as communication is a crucial element in care. The authors argue that robot designer should think of the worries of consumers relating to privacy and security – and thus ensure that robots are designed understandable and transparent.

Therapeutic chat bots are according to Fiske et al. (2019) relying on the fact that patients share their most intimate and private information in order to work. This not only does this affect the dimension of psychological privacy – by exposing thoughts and feelings to the robotic agent –, but it affects social privacy as the client will have to form a relationship to the virtual therapist. Calo (2011) points out the possibility of owners to configure social robot to certain situations with social meaning to them – situations that could be perceived rather controversial – while being recorded and those records being preserved. Related to the possibility of configuration, Calo (2020) argue that sensitive personal information could be revealed from analyzing settings and usage statistics, which the author calls »setting privacy.« Kaminski (2014) finds that robots in the home, might challenge boundary management, meaning that the users of the robot are not able to manage social accessibility – the robots can for once cross physical boundaries and if they encourage a social relationship.

Manipulation

The number of publications that deal with active manipulation of users is relatively low: (i) Calo (2011) points out the danger of anthropomorphic robots, (ii) Rueben et al. (2018) point out manipulation as one of the privacy impacts of robots, and (iii) Bartoletti (2019) state that trust towards the collection of data is decreasing as scandals about online manipulation get known. Therefore it seems like the possible threat of manipulation of users by care technologies are not yet present much in the current literature. This aspect will need further consideration in the future, as more privacy infringements get public attention, such as the Cambridge Analytica scandal or the Pegasus spyware affair. Those scandals could potentially lead to higher awareness regarding the possible manipulation by robots.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

4.3.4 Privacy Paradox

Only a few publications deal with the topic of the »privacy paradox,« among them Lutz and Tamò (2015) which point out the basic meaning of the paradox, that while people are concerned about privacy, they do not adapt their behavior accordingly. Rueben et al. (2018) also mention that people are quick to give up their standards regarding privacy, which is another problem concerning care robots. Novitzky et al. (2015) points out the problem of dependency which can come from AAL technologies, finding that this over-dependence could also drastically reduce the validity of informed consent given. The latter example shows that by creating a dependency – wittingly or unwittingly – patients might be forced to accept whatever agreement regarding their privacy, that is presented to them.

4.3.5 Emerging Technologies

Felzmann et al. (2016) point out the advantages that big data analytics would bring especially in the health care sector, and in this regards also that data gathered by robots from elderly care would add significant value. The study finds that emerging technologies play a role in the analytics of big data, such as cloud computing, cloud robotics and IoT will increase the risk for security breaches, as there are more devices involved – e.g. if a robot is connected to a smart fridge to order food for the user –, and also as the data is stored in a cloud for processing. Lutz, Schöttler, et al. (2019) point out the black box problem, cloud computing and the implications of algorithms working with big data, which can lead to obscure handling of sensitive information. Eduard Fosch-Villaronga and Albo-Canals (2019) find that cyber-physical nature of social robots complicates security and thus threatens privacy, as physical as well as digital security has to be ensured, with the complexity increasing as new technologies such as cloud computing and blockchain are used.

Automated Decision-Making

Thorstensen (2018) investigates the privacy impact of AAL technologies and how automated decisions regarding health made by the system could be in conflict with the GDPR which demands consent in such situations – which potentially could be a conflict of health and privacy. According to Thorstensen in order to give the required informed consent to make automated decision, the patients would need to understand what they are exempting – which, especially when machine learning algorithms are used, might be very complicated as it involves large amounts of data and the decisions are inscrutable to humans. Schomakers and Ziefle (2019) on the other hand, conducted a study on the privacy perceptions with AAL technologies where they found that respondents were not worried about automated decisions made by the technology.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

AI, Big Data and Machine Learning

Fiske et al. (2019) point out the advantages of using AI based services in mental health applications: they can be used for early detection of mental health concerns, for reaching risk groups which will not go to psychotherapy due to the stigmata that goes with it, such as war veterans, and they have the potential to reach people in countries where there is a lack of resources for conventional therapy, among others. Also, Bartoletti (2019) point out that the usage of AI in healthcare brings promising developments, such as identification of diseases before the manifest, spotting of genetic disorders and also improving the hospital experience for patients, and reducing waste and inefficiency likewise. Bartoletti investigate the broader concept of AI and which challenges it brings in the healthcare sector – which is of urgent importance, as care robots depending on the degree of autonomy they have, will in one or another way have implemented AI. According to Bartoletti public trust towards data collection is decreasing, as scandals about behavioral advertising and online manipulations get known; still data is gathered in all aspects of our life: via our smartphones, tracking of online movement – our data is furthermore used as a currency to access entertainment and other services at no cost. Bartoletti argue that healthcare data contains very sensitive, private information, whilst being vital to get the most potential from AI and data analytics applications in the health sector. In regards to privacy, Bartoletti (2019, p.9) points out a contradiction »the key underlying issue is that 'big data' challenges the core principle of privacy – which is to collect as little data as possible,« and the author suggest mandatory data privacy impact assessments on the development of algorithms, to assess risks or privacy harms, and to identify privacy enhancing technologies needed to protect patient data. Ienca and Eduard Fosch-Villaronga (2019) point out that with AALs technologies, large amounts of data from monitoring patients are collected; which requires that the patients are aware of which data is collected, that they can give informed consent, that no unauthorized access to the data should be possible and that it has to be clear who is the data controller and who is the data processor, as in a cloud robotics environment this might remain unclear. Moreover, Ienca and Eduard Fosch-Villaronga elaborate on wearable devices where there also massive amounts of data that can be collected, that exceed e.g. images from monitoring by cameras, such as pulse rates, blood pressure or sugar levels.

Social robots will often use AI technologies to interact with patients (e.g. Rincon et al., 2019), as well as to learn and adapt from these interactions. According to the European Commissions' High-Level Expert Group on Artificial Intelligence (AI HLEG) those records may allow to infer sexual orientation, age, gender, religious and political views apart from the user's preferences and the data originally provided.[19] Adequate data governance that covers the quality and integrity of the data used is therefore necessary, also in context of care robots, to protect psychological and informational privacy. Schulz et al. (2018) also discuss the usage of machine learning technologies in combination witch care robots, and the consequences it has for privacy, namely that the robots' algorithmic capabilities

[19] https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai, last accessed November 26, 2021

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

may be based on training data they collected from several patients. If a patient now would like to remove their data, this also has an effect on the training data used for the algorithm – Schulz et al. raise the question whether it would be technically possible to reteach the algorithm, or if then again new data needs to be added. Also, Schulz et al. ask whether data that has been removed from the actual training data, but remains in the algorithmic behavior, is actually deleted. According to Vallverdú and Casacuberta (2015) it is possible to identify individuals by overlapping different data sets, even if the health data was anonymized. They find that trust will be important, and will be a deciding factor for people if they would give personal health data to medical machines. As privacy should be investigated in context, Vallverdú and Casacuberta find that there are some elements missing or overdeveloped when the context moves from the real world to the internet. Moreover Vallverdú and Casacuberta argue that traditional conditions no longer hold for privacy in autonomous AI agents, as they illustrate by pointing out the differences in (i) how identification is achieved, as in the real world the default is to be anonymous but in the cyberspace the norm is to be identified, (ii) on who can be listening, as in the real world there are usually no listeners but in cyberspace anyone could be listening, and (iii) that de-identifying records works in the real world, but with an abundance of online databases the records can be traced back. Li and T. Zhang (2017) projects that AI technologies will be helpful in health care applications, to monitor daily life, sleep time and the diet, but warns that with intelligent methods attackers might get access to private information illegally. In relation to AI, Li and T. Zhang point out that big data is the driving paradigm, bringing the following challenges for privacy: (i) usage of personal information for commercial purposes by companies, (ii) privacy in cloud computing, as many AI applications are executed through this technology and (iii) extraction of personal information from seemingly unrelated data with knowledge extraction techniques.

Frik et al. (2019) conducted semi-structured interview with 46 older adults regarding privacy and security threats they face with emerging technologies which showed that some elderly have a limited understand on how profiling via usage of smart devices works, but they seem to be aware of fraud, scams, identify thefts and the like, and thus seem concerned about their information being sold and used for secondary or malicious purposes. Frik et al. point out the importance of transparency relating to the collection of data, and mention also that there is already a lack of control about video and audio data captured by smart devices in households such as smart TVs, voice assistants, or home-control systems.

Li and T. Zhang (2017) on the other hand, find that AI technology could also enhance security of systems and protect privacy, by using pattern recognition and machine learning to detect privacy invading behaviors.

Cloud Computing and the Internet of Things

Lutz and Tamò (2016) point out the dangers that cloud robotics and big data analysis brings, and also mention that those technologies are more often used with the rise of

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

IoT technologies. Rueben et al. (2018) also discuss the different forms of storing and processing in connection with care robotics, which are (i) onboard, when data is only processed on the hardware of the robot, (ii) local which means that there is another device necessary, such as a computer or smartphone where the processing takes place, and (iii) external, which refers to cloud computing – which they say is especially a concern to privacy, as it also opens the possibility for external people to access and control a robot. Eduard Fosch-Villaronga and Roig (2017) also find that large amounts of data that are collected by robot sensors will be processed on cloud platforms, and thus the data protection issues also need be addressed in those environments.

Theoharidou et al. (2017) points out that smart home healthcare devices range from simple devices to intelligent devices, which come with different challenges for privacy. The authors call for best a practice guide regarding privacy in health care smart homes, which should also take into account emerging technologies such as cloud technology and the Internet of Things (IoT).

In the context of an IoT future, with more and more devices being connected to the internet, Denning et al. (2009) point out the possibility of a multi-robot attack – even if a robot is considered secure, but there are other robots in the household, together using minor security gaps they could be used in malicious ways. The security gap of one device which could be considered no danger, could be used to control another device such as a robot for malicious activities.

Challenges of Emerging Technologies for Regulation

Kaminski (2014) summarizes that legally speaking, one of the most notable properties of household robots is the ability to process information unpredictably, such as it is the case with machine learning algorithms. Pagallo (2013) point out that today's legal systems will be challenged by robots, as public as well as private information will be spread to cloud servers. The author finds that such decentralized network-centric applications, which are common in ubiquitous computing environments, will be a threat to informational privacy of customers, and will make it harder to identify the source where a potential legal injury has originated. Also, Simshaw et al. (2015) find that emerging technologies, might cause unprecedented legal challenges for the protection of patients' safety, security, and privacy; and they propose that policies and practices by healthcare institutions should be reviewed regularly, and that security and privacy by design principles should be encouraged in the design of care robots. Ishii (2019) discuss three aspects of problems of AI and legal data protection: (i) digital profiling is used as indispensable technology to make automated decisions, which could, if the data misrepresents the individual, or if intimate data is revealed, lead to a privacy violation of the individual and to a unjustified evaluation of the individual by others; (ii) the supporting technology to AI, such as robots, can sense the environment and thereby collect a large amount of data, such as location, behaviors and images from the home of the individual; (iii) due to the nature of robots as a kind of companion, people might be more willing to share intimate details of their private lives with them.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Legal frameworks on privacy and data protection will be challenged by robots, as their behaviour, when using AI and machine learning technologies, depends on individual interactions with humans (Pagallo, 2013). Ishii (2019) studies the challenges for privacy and data protection that AI and machine learning technologies bring with them, which many robots use or will use. The publication by Ishii specifically focuses on the regulation in the EU (GDPR), the United States (Consumer Privacy Bill of Rights Act) as well as Canada (Personal Information Protection and Electronic Documents Act) and Japan (Act on Protecting Personal Information), pointing out the weaknesses and strengths in the protection of data, and in detail the »decisional privacy« meaning the ability to control how information about oneself is shared. The decisional privacy is similar to the aspects of control over how information is shared which is brought up by Burgoon (1982) in the description of informational privacy. Ishii argues, that the unpredictability of AI is the main problem for regulation: while the GDPR gives the individual control over data, with e.g. the »right to be forgotten,« such matters can be inscrutable when machine learning in combination with IoT technology and the capability of sensing is involved, which is the case for care robots. With deep learning Ishii point out, all kinds of information are extracted even without human intervention. Kaminski (2014) also points out the legal challenge when information is processed unpredictably. In order to protect privacy, Li and T. Zhang (2017) suggest legal frameworks that should regulate and as appropriate limit the capabilities of AI. Furthermore, Simshaw et al. (2015) find that emerging technologies, might cause unprecedented legal challenges for the protection of patients' safety, security, and privacy; and they propose that policies and practices by healthcare institutions should be reviewed regularly, and that security and privacy by design principles should be encouraged in the design of care robots. Vallverdú and Casacuberta (2015) point out the problem of health data and big data processing, where they find that it is unlikely that a person would actually accept a third-party database to store personal information about oneself; nevertheless this might be the case with automated data gathering.

Consideration of Emerging Technologies

As it can be seen in Figure 4.4, the impact of emerging technologies on privacy issues is considered more often in publications of the recent years. Emerging technologies are a hot topic in this discourse starting in 2013, with up until 2019 around half of the publications mentioning those technologies in relation to the implicated privacy issues. For further research it will therefore be important to keep those rapidly occurring technology changes in mind.

4.4 Privacy Violation Mitigation Strategies

So far the dimensions of privacy addressed in literature were discussed (Section 4.1), followed by the notions on how privacy is affected by care robots (Section 4.2) and the

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

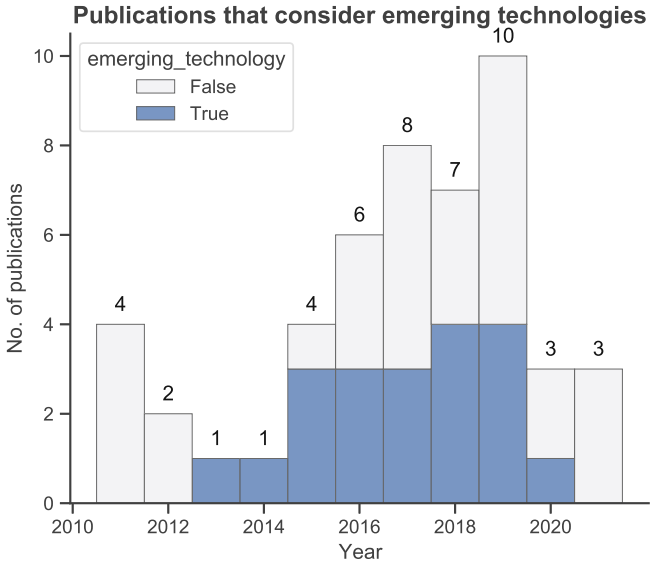


Figure 4.4: No. of publications that consider emerging technologies

concerns that authors raise (Section 4.3). The following section focuses on strategies to mitigation the impact on privacy by care robots that were proposed in literature.

Mitigation strategies identified by Lutz, Schöttler, et al. (2019) are among others transparency, the control over personal data, data minimization especially in context of the GDPR, informed consent and anonymization of data. Lutz, Schöttler, et al. list the most noted concepts to deal with privacy infringements as the »Privacy by Design (PbD)« approach, the »contextual integrity« established by Nissenbaum (2004), as well as Fair Information Practices (FIPs). Rueben et al. (2018) promote education and experience with robots over time, and to inform about rights such as the GDPR. Possible privacy violation mitigation strategies are according to Jecker (2020) encryption, the anonymizing of data and granting more control to users over their data; the latter could unfortunately lead to so-called »oversharing,« as people might take greater risks. Ishii (2019) points out the potential of the *SmartData* concept, where the data should protect itself using virtual cognitive agents, while at the same time doubting the technical feasibility. Another mitigation strategy Ishii points out are »no-go zones« which define sets of data that require consent or prohibit use. Regarding privacy risks, Novitzky et al. (2015) point out that the pervasiveness of AAL poses certain challenges, but they mention privacy-preserving video technologies as a mitigation strategy. Such a technology would for example be shape extraction. Moreover Novitzky et al. find that PbD, Security by Design and Safety by Design should should be imperative. Lutz and Tamò (2015) propose the following design considerations: (i) transparency, (ii) predictability, (iii) opt-out mechanisms or kill switches, and (iv) privacy by design next to generally minimizing data, anonymize and providing informed consent; moreover they argue that privacy impact assessments

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

(PIAs) provided by regulators are useful to guide designers. Lutz and Tamò distinguish between two approaches to implementing privacy protection measures into robotic design: bottom-up, meaning that the engineers implement the privacy measures when designing the devices, or top-down, meaning that the regulators are defining laws that have to be followed, where they name PbD as example. Definitely, Lutz and Tamò argue that privacy should be considered in advance and not in retrospect. As mitigation strategy, Schomakers and Ziefle (2019) suggest that users are able to decide with whom and what data is shared, and to implement AAL systems in a modular fashion, so certain parts of the system can be switched on and off – an important approach also to account for user diversity, which the study also found to be important, as the privacy perceptions are very individual. Thorstensen (2018) mentions other scenarios for preserving privacy in a smart home, such as the privacy keyfob, a hardware device which has build-in authentication mechanisms and allows to take privacy precautions. Alaiad and Zhou (2014) recommend the use of privacy seals issued by authoritative third-party organizations, and the use of advanced encryption technologies. D. Yang et al. (2021) studied different robot behaviors, which could could have an effect on the perceived privacy infringement: (i) gaze (closing eyes or turning around), (ii) distance (social space – 2 m distance, or public space – 4 m distance), and (iii) clarity in expressing intent (auditory signalling or visual signalling). The study concludes that all behaviors can reduce privacy concerns of users. They found that most effective is a combination of all three behaviors, but already one behavior could be sufficient. Draper and Sorell (2017) found that the perception of privacy violation depends on the reason for recording, the means of recording, the subject of the recording, who has access, and on whose authority; and that medical confidentiality helps to establish trust and minimize privacy concerns. Li and T. Zhang (2017) find that AI technology could enhance security of systems and protect privacy, by using pattern recognition and machine learning to detect privacy invading behaviors.

4.4.1 Transparency and Trust

Schafer and Edwards (2017) propose the avoidance of deceptive or misleading design of robots, in order to follow a transparency by design approach – as they find that robots have the potential to be a significant threat to our privacy. The authors find that robots challenge our privacy protecting behaviors, as we might not be aware of being filmed or sensed otherwise if the design of the robot suggests e.g. the eyes of the robot are where the cameras are located; at the same time, they also point out a conflict between safety and privacy: e.g. for self-driving cars the sensors should be hidden as vandals might cover them with paint if they can easily find them, causing a significant safety issue. Furthermore, according to Schafer and Edwards, robots should be not only transparent in appearance, but in their algorithmic functions and their ability to collect and share data. Designing the robot so that it is clear what data is collected, is also brought up in experts interviews conducted by Lutz, Schöttler, et al. (2019). D. Yang et al. (2021) found that the robot behaviors (i) gaze, (ii) distance and (iii) clarity in expressing intent improve transparency, which makes the robot more understandable for humans. Lee et al. (2011) suggest in their study that as long as the robot informs users that they are recorded, they

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

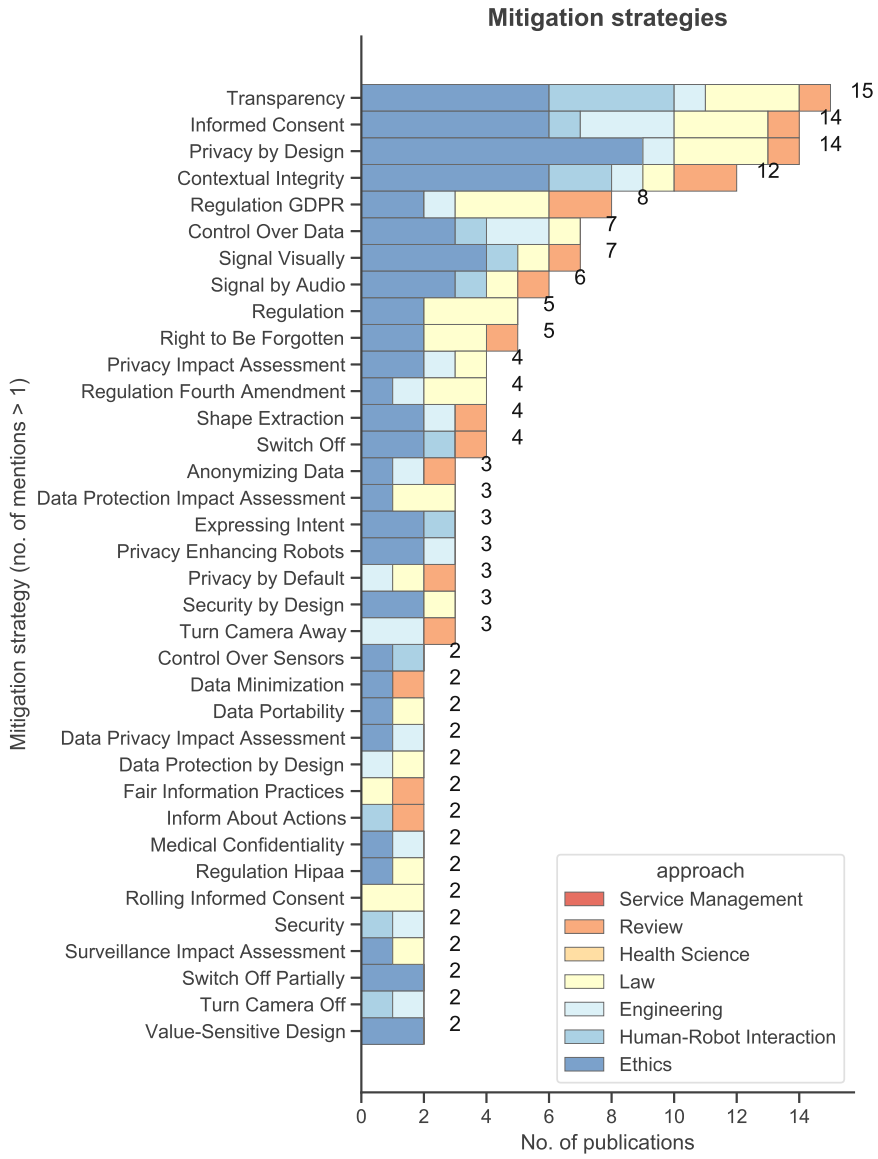


Figure 4.5: Mitigation strategies discussed in literature

are not concerned about it, but they are less comfortable if there would be accidental recordings they are not informed about, and they also expressed concerns if recordings are used out of context, such as to track a user's location or routines unwittingly. Lutz and Tamò (2016) find that the social privacy aspect should not be neglected in care robotics, as communication is a crucial element in care and argue that robot designer should think of the worries of consumers relating to privacy and security – and thus ensure that robots are designed understandable and transparent. Schulz et al. (2018) find that making patients aware of the robots capabilities and giving them possibilities to negotiate

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

privacy is crucial, but they find there is no solution which provides all answers. Reinhardt et al. (2021) found in a survey with 1090 participants, that most felt uncomfortable if the robot was able to predict their location; they therefore argue that transparency and explainability are to be further investigated to influence the comfort level regarding privacy. Rueben et al. (2018) point out that transparency is important when it comes to whether a robot is recording, and what it is recording; moreover they point out the problem of patients that are not capable of understanding what is happening anymore. Draper and Sorell (2017) found that whether a recording is perceived as a threat to privacy, is depending on the reason for recording, the means of recording, the subject of the recording, who has access and on whose authority. This finding also points to the importance of transparency regarding the processing of video material and data. Frik et al. (2019) conducted semi-structured interview with 46 older adults regarding privacy and security threats they face with emerging technologies. Transparency, i.e the lack or such, the study points out is a major concern for the participants relating to data collection the control of recordings by smart devices. Heuer, Schiering, and Reinhard Gerndt (2017) point out that awareness for the privacy risks of robots is important for users and thus for the acceptance of the technology, which asks for transparency and a careful assessment of issues related to privacy that are linked with the functionalities of the robot. Transparency, Heuer, Schiering, and Reinhard Gerndt point out, is needed, as to address the users concerns of the collection of personal data, and also regarding what for and why sensors are used. Finally, Heuer, Schiering, and Reinhard Gerndt point out that those for whom social robots will be especially targeted – older adults as well as children –, are also those that might have the most difficulties regarding the awareness of the full risks that they implicate. Transparency is also important in the design for setting privacy preferences. Lutz and Tamò (2015) argue that privacy configurations should not be complicated, but easy for users to understand.

Frik et al. (2019) found that the participants of their study believe medical staff in general to more trustworthy when they have to deal with entering medical data in online portals, which is a more common phenomenon among older people than younger. A survey by Fernandes et al. (2016) found interesting aspects about the perceived intrusion to physical privacy and also the fear of unwanted disclosure of personal information. By preferring the robot to turn away, the participants of the survey conducted by Fernandes et al. implicitly voice two concerns connected to trust, namely (i) they do not trust the robot to stop recording – and they can also not enforce control over whether it is recording or not, and (ii) they do not trust the robot to store and process the recording secure and free from interventions by unwanted parties. While Poulsen and Burmeister (2019) found that the most respondents thought of the value-sensitive decisions (real-time decisions to intervene with patients based on their value priority list) of the robot in a good manner, but also that to fully trust the robot's decision they would need to know how it derived to it's decision – so the robot would need to be transparent. Moreover, Poulsen and Burmeister found that 82% of the respondents in their study also would prefer the possibility to intervene in the robot's decision. Huber and Camp (2017) discuss ethical aspects in the design of smart homes, and they find that transparency about what

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

data is recorded should not only be limited to mentioning the technologies used, but access to the actual data collected. Vallverdú and Casacuberta (2015) find that trust will be important, and will be a deciding factor for people if they would give personal health data to medical machines.

Schafer and Edwards (2017) suggest that privacy protecting human behaviour might lead to a conflict between the robot and the human. Schafer and Edwards argue, the robot might misinterpret the situation due to those protective behaviours and might become vulnerable or even a danger to others, particularly when using machine learning. However, if robots have hidden sensor capacities they could even subvert these behaviours – therefore Schafer and Edwards suggest a transparency duty concerning sensor capacities. The authors are in favour of a compromise, where humans are giving information to the robot that is required to operate safely – as an alternative to »gaslighting« the robot, even if it intrudes privacy – while in return robots should be built with open sensor capacities. Schafer and Edwards conclude that sensory capacity of robots should be transparent, as then the user has a choice whether to cooperate or not; if the non-cooperation would cause harm, the authors leave open for discussion under what circumstances a robot should anyways be allowed to gather some data for the safe operation of the machine.

4.4.2 Informed Consent

Regarding informed consent, Ienca and Eduard Fosch-Villaronga (2019) point out that it should be given in the form of a »rolling« or »ongoing« consent, which can be withdrawn anytime; and they specify three possible ways for patients with dementia: (i) direct consent, for patients with the according cognitive capacity; (ii) by advanced directives which are given by the patients in advance where they define future decisions; and (iii) through a proxy, e.g. a family member, which were previously chosen by the patients. Also, Reinhardt et al. (2021) propose informed consent solutions, while also they found that respondents would prefer no sensitive data to be stored, except if their utility is higher than the concern of the users. Sedenberg et al. (2016) propose dynamic consent, which can be changed over time; and they recommend the user is given choice to direct and control the robot information system, e.g. choosing where, and how long data will be stored. Also, Eduard Fosch-Villaronga, Tamò-Larrieux, et al. (2018) found in their workshop on ethical, legal and societal (ELS) implications of social robots, that the concept of privacy would have to evolve around technological change and they proposed dynamic consent forms, that pop up more frequently to ask if certain data can be shared and processed – as an alternative to giving one informed consent at the beginning of usage of the robot. Blake (2019) suggests the concept of informed consent to respect the patient; it includes (i) an explanation of the purpose of the robot in their care, (ii) information on the developers and operators of the robot, and what it's sensory, physical etc. capabilities are and finally (iii) a warning about risks and burdens of the technology to make an informed decision. The better a patient understands a robot, the better one is protected against privacy breaches (Blake, 2019). Felzmann et al. (2016) propose to implement informed consent in regards to medical gathering of data. Rueben et al. (2018)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

propose a »opt-in« approach, regarding the personal information that should be shared, meaning that users have to give their consent explicitly if they want to share information.

Validity of Informed Consent

Ienca and Eduard Fosch-Villaronga (2019) find that agreements and contracts made through telepresence robots need to unambiguous and clear, to avoid any abuse. Lutz and Tamò (2015) point out that with data collection becoming more ubiquitous in online applications, consent to the collection of data is often abused to gain access to location, personal information our to our contacts, for example in smartphone apps – as we get more used that those applications require this consent. Novitzky et al. (2015) point out that the hi-tech nature of AAL technologies technologies might make it difficult for dementia patients to understand what thy are giving their consent to, thus questioning informed consent as a mitigation strategy and call for further analysis on the issue. A. Sharkey and N. Sharkey (2012) question whether a patient in mental decline can give consent, but also whether their relatives should be allowed to do so. Similarly, Thorstensen (2018) also discusses how to deal with informed consent with patients of declining cognitive capabilities, mentioning »rolling informed consent« where the consent is asked repeatedly, taking into account the competence of the person to participate in the decision and also telling that they can opt out every time. Further Thorstensen point out that at some point, somebody else than the patient with declining cognitive abilities will be in charge to set the privacy levels of the patient. Regarding AALs technologies, Ienca and Eduard Fosch-Villaronga (2019) point out that large amounts of data from monitoring patients are collected; which requires that the patients are aware of which data is collected, so that they can actually give informed consent. A similar insight has been gained by Thorstensen (2018), which found that in order to give the required informed consent to make automated decision for a robot, the patients would need to understand what they are exempting – which, especially when machine learning algorithms are used, might be very complicated as it involves large amounts of data and the decisions are inscrutable to humans. Novitzky et al. (2015) found that over-dependence to AAL technologies could also drastically reduce the validity of informed consent given. Moreover, Novitzky et al. found that not only has the the consent to be given by a primary user, as if such technologies are used with co-habitants their consent would be needed as well.

4.4.3 Privacy by Design (PbD)

Cavoukian (2010) defined the seven principles that are the basis of the Privacy by Design (PbD) idea as follows:

1. Being proactive instead of reactive in terms of privacy invasive events.

2. Deliver the maximum degree of privacy as default, by protecting personal data automatically, the individual does not have act in order to protect their privacy.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

3. Privacy is embedded into the design, not added after the design, thus making it an essential component of the functionality.

4. Avoid unnecessary trade-offs to protect privacy, but instead create a positive sum at full functionality.

5. Throughout the lifecycle privacy is protected and at the end of the lifecycle the data is securely destroyed.

6. Visibility and transparency is ensured, the technology is operating as promised and the operations remain transparent for users and providers to enable independent verification.

7. The interests of the individual are kept highest by the architects and operators, not only limited to privacy but also to appropriate notice and user-friendly options.

In the PbD approach, (Pagallo, 2013) describes, personal data collected by robots should be automatically protected as a default; data protection should be proactive, rather than reactive, and the used mechanisms have to be transparent for both, the robotic users and the providers. Legal frameworks on privacy and data protection will be challenged by robots, as their behaviour, when using AI and machine learning technologies, depends on individual interactions with humans (Pagallo, 2013). Simshaw et al. (2015) propose that policies and practices by healthcare institutions should be reviewed regularly, and that security and privacy by design principles should be encouraged in the design of care robots. Ishii (2019) favor the PbD approach to preserving privacy – which could be operationalized e.g. with de-identification or biometric encryption – the most, as it comprehensive and moreover, it is internationally recognized by the EU, USA, Canada and Japan. Privacy should be considered before the design of robots, and that legal frameworks need to be taken into account (Lutz and Tamò, 2016; Lutz and Tamó-Larrieux, 2020). Eduard Fosch-Villaronga and Albo-Canals (2019) point out that developers of AI or other robotic applications have to make sure to implement PbD, the right to be forgotten, as well as data portability and transparency, which are part of the GDPR. Armbrust et al. (2011) argue that an assistive should only collect as much data as absolutely necessary, specifically excluding information about the daily schedule of the individual – this should only be stored on the robot –, images and videos should only be accessible by the caregiver in case of emergency, and not stored. By introducing these goals, Armbrust et al. also show their concern for informational privacy, which they aim to mitigate by limiting the collected data to a bare minimum. Armbrust et al. suggests that caregivers only get access to the home (physical privacy) in case of emergency, and also they can only access information about the client (informational privacy) in case of emergency. Other authors that also propose PbD as a privacy violation mitigation strategy in their publications found in the literature review, are Huber and Camp (2017) and Ienca, Wangmo, et al. (2018).

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Control over Data

Schomakers and Ziefle (2019) found it to be evident that control over data is the most important element, and the control whom to entrust their data – which is depending on how sensitive the data might be. Eduard Fosch-Villaronga, Tamò-Larrieux, et al. (2018) did a workshop on ethical, legal and societal (ELS) implications of social robots, where the group had a focus on discussing data processing, suggesting three possible scenarios: (i) end users give permits to collect data, (ii) end users identify the data that can be collected, but it is required to be anonymized and (iii) end users prohibit data collection completely. As Eduard Fosch-Villaronga, Tamò-Larrieux, et al. write, the group argued that most likely the second scenario (ii) will be the case.

Data Protection

In a focus group experiment, Draper and Sorell (2017) found that the security standards and the storage duration on the data-storage is a decisive factor for whether video material from monitoring or collected data is perceived as privacy infringement. Armbrust et al. (2011) propose to use encrypted data storage, and only Secure Sockets Layer (SSL) secured network connections, respectively the video communication platform Skype as it is secure and encrypted. A. Sharkey and N. Sharkey (2012) raise questions over the duration that data shall be stored, and who shall be allowed to access it, especially if the patient can not give consent. Felzmann et al. (2016) propose to apply good data protection practice, which aims for minimizing data that is stored long term, and a general reduction of data storage in accordance with PbD. Ienca and Eduard Fosch-Villaronga (2019) analyzed AALs technologies, social robots or telepresence robots and wearable devices and suggests a PbD approach where all possibilities of data protection and potential privacy infringements are considered.

Impact Assessments

Bartoletti (2019) suggest mandatory data protection assessments (DPIAs) on the development of algorithms, to assess risks or privacy harms, and to identify privacy enhancing technologies needed to protect patient data. Eduard Fosch-Villaronga and Roig (2017) promote using a risk-based approach to assess the impact of robots, which not only focuses on damage but every potential and actual adverse effect. According to them, risk-based approaches are already used in an array of sectors in the form of PIAs, privacy impact assessments (SIAs) and environment impact assessments (EIAs). Also Ishii (2019), points out PIA, similarly as incorporated in the GDPR as important tools, which are incorporated in the PbD approach. Moreover, Eduard Fosch-Villaronga (2019) point out that DPIAs have already become mandatory with the GDPR. Eduard Fosch-Villaronga and Albo-Canals (2019) propose to implement a robot impact assessment (RIA) – in contrast to single impact assessments on data protection or surveillance –, to implement a process to produce applicable robot guidelines and to create a code of conduct – principals and values that have to be respected by robot developers.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Criticism on the Privacy by Design Approach

Lutz, Schöttler, et al. (2019) also found criticism to whether PbD would be feasible as a pre-programmed solution might not fit the user behavior, and that rolling informed consent to extended amounts of data collection might not be possible. Thorstensen (2018) finds that the maximum privacy setting on new devices, which is required in the PbD approach, might conflict with requirements of those who already are living in a smart home when activating a new device in their home which could be prevented from performing health critical monitoring due to the privacy setting.

4.4.4 Contextual Integrity

One concept that is often mentioned in connection with care robots and data collection in general is the concept of contextual integrity established by Nissenbaum (2004), which argues that privacy should be protected according to norms of specific contexts.

> According to the theory of contextual integrity, it is crucial to know the context – who is gathering the information, who is analyzing it, who is disseminating it and to whom, the nature of the information, the relationships among the various parties, and even larger institutional and social circumstances. It matters that the context is, say, a grocery store as opposed to, say, a job interview or a gun shop. When we evaluate sharing information with third party users of data, it is important to know something about those parties, such as their social roles, their capacity to affect the lives of data subjects, and their intentions with regard to subjects. It is important to ask whether the information practice under consideration harms subjects; interferes with their self- determination; or amplifies undesirable inequalities in status, power, and wealth. (Nissenbaum, 2004, p.137)

Applying the theory of privacy as contextual integrity by Nissenbaum (2004), Sedenberg et al. (2016) argue that privacy issues must be addressed in context, e.g. what are the norms when therapeutic robots are moved from hospital settings into personal spaces. On the other hand the authors propose the application of the FIPs (see Gellman, 2019), which protect informational privacy, as well as emphasize the principles of transparency, access, privacy controls, integrity and data use protections. Lutz and Tamò (2015) argue that contextual integrity is useful to adapt to the different context where robots might collect data; which is important in regards to informational privacy (Lutz and Tamò, 2016). Jecker (2020) promotes regulatory frameworks derived from contextual analysis e.g. the requirements for a regulatory framework would have to consider the different situations during a pandemic, such as that the higher degree isolation makes human users more vulnerable to abuse. Such a contextual approach could according to Jecker also be applied in situations where physical security are at stake – e.g. the conflict of keeping the dignity of older adults, while their informal caretakers (such as their children) have the ability to check on them. Moreover, Jecker finds that context analysis could identify the regulatory protections needed when robots are connected to the internet and open the possibilities for hackers to access door locks, security systems, etc. which not only is a violation of privacy but a safety issue. Kaminski (2014) finds that robots in the home, might cause a violation of contextual integrity – meaning that an

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

information revealed in one specific context will not be transferred into another context, where other social norms might apply. Vallverdú and Casacuberta (2015) point out that privacy should be investigated in context, and they find that there are some elements missing or overdeveloped when the context moves from the real world to the internet. Also referring contextual integrity, Rueben et al. (2018) propose that robots should act different according to the context; and also they point out that robots should be able to distinguish the context where it is appropriate to display information to people visiting. Another interesting aspect Schulz et al. (2018) point out, is that a patient might have different social roles, e.g. being a grandparent or being somehow involved in honorary positions, something a care robot should take into account when e.g. disclosing sensitive information regarding the health of the patient.

Sedenberg et al. (2016) point out that not only the primary user of the robot, such as an elderly person receiving care, might be affected by the collection of private information, but also family members, friends and visitors which could be unaware of the presence of the robotic agent – therefore arguing for transparency of the usage of sensors. This raises not only an issue of privacy, but concerns about the integrity of the data used for the therapeutic treatment of the person in care, especially when machine learning techniques are used (Sedenberg et al., 2016). Mistakenly collected data could interfere with an appropriate treatment Sedenberg et al. argue, and also expose sensitive information of the visitor to the owner of the robot or the robot providers. Sedenberg et al. therefore recommend the possibility for users to amend their records for inaccurate or incomplete data, hoping to maintain integrity; also they discuss who should be given access to data, especially when the users have diminished autonomy – leaving the answer open for debate. Also another study found the aspect of the violation of privacy of bystanders: Frik et al. (2019) argue that if technologies are in the same room and the users might not even be aware of it – the use of such by others causing uncomfortable feelings to the bystanders.

Nevertheless, Ishii (2019) remark that implementing contextual integrity – the complete control over personal data, as suggested by Nissenbaum (2004), is not necessarily enough to protect privacy when faced with AI and machine learning technologies.

4.4.5 Regulation

Blake (2019) conclude that regulation to ensure the quality and standards of care robots, to guarantee governmental oversight, and to inform patients thoroughly about risks and tradeoffs will be crucial to ensure that care robots will be a useful tool for society. A. Sharkey and N. Sharkey (2012) see the development of guidelines, or better legislation and value sensitive design of robots as solutions to mitigating the potential risks. Kaminski (2014) points out that introduction of household robots might be a »privacy catalyst,« that subsequently will reveal inconsistencies of the U.S. privacy law. Kaminski summarizes that legally speaking, the most notable properties of household robots are the (1) need to sense and record large amounts of data (which they also often share with third parties); (2) the ability to move independently; (3) the possibility of being attributed social meaning and (4) the ability to process information unpredictably, such as is the case with machine

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

learning algorithms. Lutz, Schöttler, et al. (2019) find that most legal scholars criticise current grey areas in the law, while they call for adaption of legal frameworks; and also that of now the most covered privacy aspect in legal frameworks is informational privacy. Other than the EU has the GDPR, Kaminski (2014) points out, the United States is lacking a holistic approach when it comes to the handling of data. Kaminski furthermore finds that under the third party doctrine of the U.S. Fourth Amendment, the data does not fall under privacy protection and is available for government meddling without a warrant, as it was willingly shared with a third party, which was also pointed out by Sedenberg et al. (2016). Pagallo (2013) found that the extend of »reasonable expectation of privacy« – which defined by the court order *Katz v. United States* – can in the field of human-robot interaction can currently not yet be foreseen. Kaminski (2014) finds that it will be challenging to courts to differentiate between privacy, permission, and trespassing; the author asks how to handle cases such as if a robot enters physically where they are not allowed, if a robot was invited physically but not allowed to record or if a robot deceived people into revealing sensitive information. Kaminski futhermore finds that existing privacy laws in the United States will have to be adapted, and proposes that FIP principles should be applied for data gathering and analysis. Ienca, Wangmo, et al. (2018) argue that patients should be allowed to legally claim ownership over their data, either personally or through a proxy.

Carnevale (2016) points out that the more robotic technologies are used in domains of disability, aging, education, healthcare, etc. the more legal norms and ethical principles will be necessary, thus also re-thinking privacy becomes crucial; and the author calls for leaving the normative approach to privacy behind and move towards an instrumental view, where privacy is a means to achieve goals. According to Carnevale the case of privacy teaches that the problem is not robots becoming more human, but the extend of legal protection of one's personal identity and integrity, and therefore calls to transform the issue of privacy from a matter of individual rights to a political challenge.

Flexible Regulation

Lutz and Tamò (2015) make their point that privacy balancing mechanisms should be developed iteratively, and propose flexible regulations which find out the ethical principles on-the-go while designing technological solutions. This approach, the authors argue, would treat ethical values as something that can be experimented with. Generally, also Ishii (2019) prefers a flexible soft law regime based on foundational principles, instead of laws targeted specifically for AI, due to the unpredictable nature of AI. Ienca and Eduard Fosch-Villaronga (2019) recommend that data-protection regulations for IATs should provide elasticity: as this would allow the maximum benefits of the technology, while preserving the privacy of patients and avoiding technological misuse; while also pointing out that too strict regulation would also impact the future technological innovations negatively. Carnevale (2016) finds that legal frameworks lose validity due to technology changes, thus to protect privacy accordingly laws have to change as robotic technologies evolve.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Care Robots vs. Medical Devices

Simshaw et al. (2015) assess care robots from a legal perspective. They summarize that in the United States currently the safety and security of medical devices fall under the regulation of the U.S. Food and Drug Administration (FDA), and the related health data is protected under the Health Insurance Portability and Accountability Act (HIPAA). Simshaw et al. argue, that for robots that are categorized as medical devices, the processing of data will be subjected to the HIPAA, while those, who fall outside the scope of medical devices will be fall under the data protection of the U.S. Federal Trade Commission (FTC), which protects consumer interests; implying that health data might be collected by personal care robots which would not get the same privacy protection standards as data collected e.g. in a hospital. Simshaw et al. propose that the collection of data by personal robots could be handled by the FTC while the further processing falls under the HIPAA privacy and security rules. Furthermore, Simshaw et al. argue, that current regulation as it is in place in the United States, also needs to be adapted, as for example the HIPAA does not incorporate proactive security and privacy protections. Ienca, Wangmo, et al. (2018) also find that security breaches in IATs are a great risk, as the do not fall under the HIPAA security standards, which applies for medial devices. Sedenberg et al. (2016) propose to implement privacy and research ethics frameworks, in order to achieve responsible and research-ready robotics in private settings. Sedenberg et al. point out that the U.S. health privacy laws, as they apply to medical devices in medical facilities, do not apply to private devices at home – at the same time the find that the home is a more complex environment where a variety of activities happens, which complicates the impact on privacy. Some more privacy complications Sedenberg et al. find is (i) the long-term data storage could lead to health data which is not up-to-date anymore, e.g. if a reading disorder has been resolved, (ii) when health data was collected in a medical context, and a patient purchases a care robot and transfers the data, said that is not protected by U.S. federal privacy law anymore, (iii) recording of participants which were not aware that they are being recorded, (iv) if private conversations of other persons than the patient are recorded unintentionally, and later exposed to the patient, and (v) the lack of a professional intermediary could lead to misunderstandings about the progress of a therapy.

General Data Protection Regulation (GDPR)

Eduard Fosch-Villaronga and Albo-Canals (2019) point out the importance of privacy and data protection, reminding that those are not merely issues to be addressed but legally binding and obligatory: for processing data of EU citizens the GDPR is valid since May 2018, regardless of which country the processing takes place. Thus, they continue, developers of AI or other robotic applications have to make sure to implement PbD, the right to be forgotten, as well as data portability and transparency, which are part of the regulation. Eduard Fosch-Villaronga and Roig (2017) point out that the GDPR actually requires legally to perform an assessment in regards to the protection of personal data. They find that performing a care care robot impact assessment (CRIA), as proposed

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

by E. Fosch-Villaronga (2015), would be helpful to mitigate risks, as it would require legislators, robot developers and the facilities handling the robot to apply regulations and standards. Moreover, Eduard Fosch-Villaronga and Roig (2017) point out that in the domain of law, privacy and data protection are currently the most relevant legal aspects for regulations and find that in robotic development, especially in HRI, those principles are not as prominently represented. Also, the authors warn that with the GDPR roboticists from inside and outside of the EU could face direct consequences if they do not consider it. Ishii (2019) remarks, that while the GDPR is very detailed, AI brings new challenges to it – which also not comparable regulations e.g. in the United States are fully equipped for. Thorstensen (2018) investigates the privacy impact of AAL technologies and how automated decisions regarding health made by the system could be in conflict with the GDPR, as it demands consent in such situations. This, according to Thorstensen could potentially lead to a conflict, as justifiable health measures would be disallowed due to privacy.

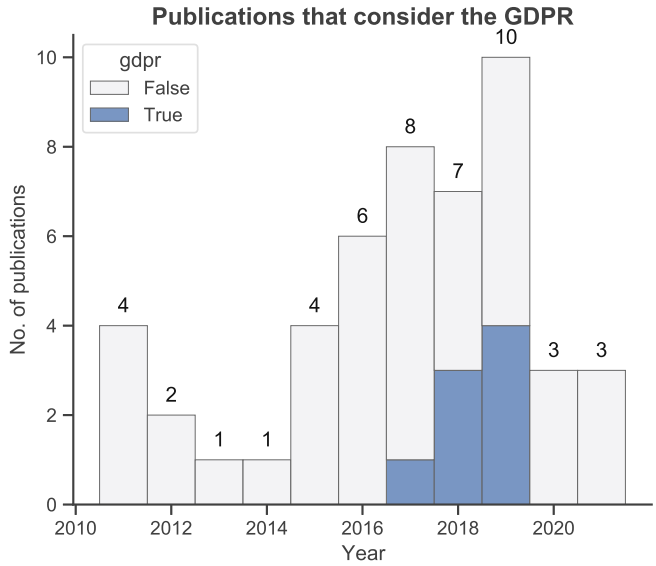


Figure 4.6: No. of publications that consider the GDPR

The number of publications that have considered the GDPR can be seen in Figure 4.6. It can be seen that in 2017, so the year after the proposal of the GDPR there has been only one publication that considered the new regulation to come, while in in 2019 already 4 out of 10 analyzed publications from that year have considered the GDPR in regards to privacy impact of care robots. From a quantitative point of view this is around half of the publications in 2018 as well as in 2019 – nevertheless it can not be stated that the implementation of the GDPR itself impacted the number of publications on the topic. Nevertheless, the GDPR did in fact impact the qualitative discussion around privacy, as it introduced mandatory requirements such as the right to be forgotten, data portability and transparency. As Eduard Fosch-Villaronga and Albo-Canals (2019) point

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

out rightfully, robot designers – not only in the EU – will have to hold up to the high standard regarding data protection and privacy, the GDPR has demanded.

4.4.6 Privacy Enhancing Engineering Solutions

Calo (2020) calls for working on »privacy enhancing robots,« which would protect homes and owners from unwanted access or surveillance – or from other technologies which have not been invented yet. Such engineering solutions to enhancing privacy are discussed in the following.

Control and Spatial Limits

Being able to control whether a robot is allowed to use sensors or not, is according to Schulz et al. (2018) unmistakable simple way to negotiate privacy, while it comes with the disadvantage of the taking away the robot's capabilities to do their job, e.g. ensuring the patients safety. Schulz et al. suggest a snooze function, which would turn on the robots' sensors after a pre-defined time again, which could again lead to a problem of finding the patient if they have moved into another room. Felzmann et al. (2016) also propose the possibility to switch off some functionalities – or also the robot as a whole depending on the patients capabilities and risk group – in order to achieve higher levels of privacy and autonomy. Lutz, Schöttler, et al. (2019) conducted expert interviews which brought up among other technological privacy solutions to be able to (i) switch off a robot and (ii) limit the space where the robot is allowed to move. As privacy enhancing feature, Van Heek et al. (2017) suggest a possibility to switch on or off the video monitoring functions.

Poulsen and Burmeister (2019) suggest robots in care should make real-time decisions to intervene with patients based on their value priority list; the values they mention are: social connectedness, independence, autonomy, respect, consent, privacy, and dignity. The authors conducted survey with 50 respondents, which were confronted with a scenario of a robot deciding whether to intrude into a room where a patient might be only partially dressed, but would need to be reminded to take medicine, where the robot makes the decision based on the observed past behavior of the patient, i.e. for a patient which values privacy most, the robot would not enter the room, but would knock on the door; if the patient would value independence most, the robot would not call for a caretaker for help but rather also knock on the door; and for a patient that valued social connectedness the most in the past (e.g. appreciates unexpected visitors), the robot would let itself in and remind the patient to take medicine (Poulsen and Burmeister, 2019).

Armbrust et al. (2011) aim to develop a care robot which minimizes the necessity of interference by caregivers, thus allowing maximum autonomy for the caretaker. This argumentation refers to the physical privacy of the robot's user – but it disregards that the robot itself can be perceived as an invasion to privacy. Seemingly aware of that fact, Armbrust et al. have also designed their care robot so that it will stay as far away as possible from the individual it takes care of; unless an emergency is detected, where

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

the robot shall be able to come to help quick – this feature is achieved by using RFID tags that the caretaker wears, that help localize and detect unusual behavior. This is an approach to ensure a maximum of safety for the user, while upholding the physical privacy i.e. to »let the user be alone,« from the robot as well from the caregivers. To allow such a robot, a high degree of autonomy is necessary, and also the capabilities to assess a situation and intervene as appropriate (Armbrust et al., 2011). Rueben et al. (2018) also propose a technical enforcement of privacy by forcing the robot to avoid certain areas. Wu et al. (2021) find that privacy perceptions are correlated with the users' level of control, thus if an older adult can also move the robot they experience a greater sense of control. Heuer, Schiering, and Reinhard Gerndt (2017) found that it is perceived important for users to be able to switch off certain features, and to ask about whether they are comfortable with a specific sensor being used or not in certain situations – and also inform whether it is necessary for a specific e.g. therapeutic treatment.

Signalize Activities

Schulz et al. (2018) suggest the usage of sensors with extended capabilities, such as to detect people through walls, should be signalled, either auditory or visually, to make the patient aware. N. Sharkey and A. Sharkey (2011) support the idea that a robot should give visual signals if recording, in order to make patients aware. Also Sedenberg et al. (2016) argue for visual or auditory signaling if a robot is recording privacy sensitive situations. Furthermore, A. Sharkey and N. Sharkey (2012) propose that robots should request a permission before monitoring, or expressing intent if they e.g. want to enter a room.

Privacy Preserving Sensors and Behavior

A proposal by Schulz et al. (2018) is to change the mounting height of sensors, such as close to the ground level, which enables to detect obstacles and people, but does not give away their identity; next to that, they consider the usage of different sensors, which do not allow the identification of people, such as LIDAR sensors instead of cameras. For technical enforcement of privacy, Rueben et al. (2018) propose among others to blur out objects (shape extraction) or to technically implement »privacy by design« e.g. by mounting the camera so low that it can not detect sensible documents and the like. Demiris et al. (2009) studied whether shape extraction, such as the replacement or removal of a person in a camera image, can impact the perceived privacy. Demiris et al. findings show that it is important for users of video monitoring applications to know what information gets recorded, what happens with the recorded information (e.g. if it will be altered), who has access to the information and what will it be used for. This experiment shows how the dimensions of physical and informational privacy are interconnected in robotic applications: while the camera recording is an intrusion of the home sphere, potentially letting strangers take part in the observation, as soon as the video is saved, it becomes data, and thus an issue of informational privacy. Demiris et al. conclude that shape extraction creates anonymity for those observed, and they state that

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

if used consequently and effectively it potentially could solve the threat of surveillance by mobile care robots capable of video monitoring. Furthermore, Eduard Fosch-Villaronga, Tamò-Larrieux, et al. (2018) brought up stimuli for privacy friendly design of robots – such as drones that navigate without cameras, and a fall detection system that works with vibration sensors on the floor, instead of camera images.

D. Yang et al. (2021) found that users are especially sensitive regarding privacy if nakedness is involved. G. Yang et al. (2018) developed a privacy detection system, with an accuracy of over 94%; basically their solution makes the robot turn the camera away if a privacy-sensitive situation is detected. Fernandes et al. (2016) found in a survey with 449 participants that about 78% consider privacy at home very important, with around a third of the respondents saying they are most concerned about nakedness. Fernandes et al. therefore designed a robot which will turn away in privacy-sensitive situations, e.g. when a person takes off clothes, thus avoiding to be exposed by the camera. While turning off the camera would also be a feasible solution to avoid recording nakedness and such, Fernandes et al. found that the preferred option is a robot detecting a situation and turning away completely, as for robot that would only stop recording there is no way to control it. It is this simple psychological effect that according to Fernandes et al. makes the difference of how people perceive their privacy loss.

Security

While Denning et al. (2009) suggest some design questions related to security and privacy, as well as regarding the planned environment and social surroundings of the robot, they do not give any specific advice how the risks those household robots pose could be prevented. Frik et al. (2019) made the important discovery, that as aging related physical abilities decline (vision, hearing, motoric abilities with the hands, etc.), persons are likely to choose easier to use technology which might be less secure. Therefore, when such privacy enhancing technology is used, it is very important to take into account that it should be designed simple and user-friendly so it can still be understood and used by the target group.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU WIEN Bibliothek Your knowledge hub

CHAPTER 5

Future Challenges

This chapter discusses the issues that need to be addressed in the future with respect to privacy in care robots. Chapter 4 has identified the predominant topics in a comprehensive literature review, now it will be highlighted which ideas need more attention and which aspects have not been addressed at all. The chapter, thus shall provide the answer to the research question **RQc** ("Which questions have to be addressed in the future?").

5.1 Social and Psychological Privacy

Concepts against the infringement of social and psychological privacy fall short in the current discussion of privacy impacts of care robots. As most publications focus on the informational respectively the physical aspects of privacy, also the mitigation strategies identifies go into that direction. While transparency is also protecting from social harm in a way, as the robot is (i) not allowed to lie about it's actions, and (ii) is clear about what it is recording and which actions it takes, and also contextual integrity proposes to differentiate social norms in different contexts, nevertheless there is room for more privacy preserving concepts. Physical privacy can be preserved with simple technological acts, as turning around, so the person does not feel watched, or shape extraction. Informational privacy can be protected e.g. with anonymization and encryption. Further research would be needed, to find if there could be engineering solutions to the problem of influencing the psychological privacy, so the values and thoughts of a person, and the social privacy. If such aspects can be exploited, users can be manipulated – a concern which was not mentioned often in the publications of the literature review. The questions to be discussed here are, whether care robots should be social at all, or if they should merely be tools; and if to what degree a robot should be allowed to lie to a person, e.g. when there would be a matter of safety that would require it. A social robot would be a constant influence on a person's thoughts, while it could be wanted e.g. to decrease loneliness, it has great potential for being maliciously used.

Burgoon (1982) found that individuals perceive less privacy intrusion if they are able to render the invading entity as a non-person, such as persons do with servants. Robots have great potential to act as non-persons, as it is a decision that can be made in the design of the robot. Nevertheless, it could also be used maliciously, e.g. if a robot then hides sensory capabilities which would better understood if the robot has a anthropomorphic appearance. It was also found that medical personnel, which are strangers, are more trusted with sensitive health information than informal caregivers such as relatives (e.g., Draper and Sorell, 2017). This contradicts Burgoon, as the author stated that relatives are perceived less of a privacy threat. Another aspect which the current literature on care robots does not address much, is whether users would create a social bond even with the machine, and thus allowing the robot to be in a social group where secrets are more willingly shared, as Burgoon described. Related to that, Burgoon wrote that one's sense of identity can be influence by another individual. The literature review did not result in knowledge whether the presence of care robots would have an effect on patients, and thus would affect psychological privacy in this aspect. Moreover, the extreme form of psychological privacy harms, which is according to Burgoon excessive stimulation that could lead to annoyance, is not discussed. This last aspect should be investigated in future research, as it is very likely that a robot with the duty to take care of a person's health might cause annoyance if the level of stimulation is too much. Furthermore, Burgoon brought up the »stranger-on-the-bus phenomenon,« where a person shares intimate details with another person who is a stranger, as they experience a sense of anonymity. This phenomenon, related to informational privacy, was not brought up in the literature review. It is nevertheless possible that robots are perceived as strangers, and thus intimate information is shared, while the robot will process and store this information.

5.2 Use of Emerging Technologies

While most authors point out the dangers that AI in combination with machine learning technologies bring for the future of privacy (e.g., Ishii, 2019), Li and T. Zhang (2017) point out that AI technology could actually enhance security of systems and protect privacy by using pattern recognition and machine learning to detect privacy invading behaviors. This approach sounds interesting and promising. As the development of emerging technologies is likely to be unstoppable, they should be used specifically to create valuable benefits for privacy, instead of diminishing it.

5.3 Limited Insight into Wearable Smart Devices

Many publications implicate the usage of wearable devices, e.g. for taking health related measurements, but no particular focus is put on examining those, and their respective impact to privacy. For example, a simple way to gain privacy would be to detect movement information about a patient not through video surveillance, but through, say, a smart watch. The patient could simply take off the watch to be free from surveillance - but

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

this again raises conflicts between safety and privacy, as well as how such situations should be handled for patients with cognitive decline. Further research into privacy violation mitigation strategies based on wearable technology could be an enrichment for the discussion of the privacy impact of care robots.

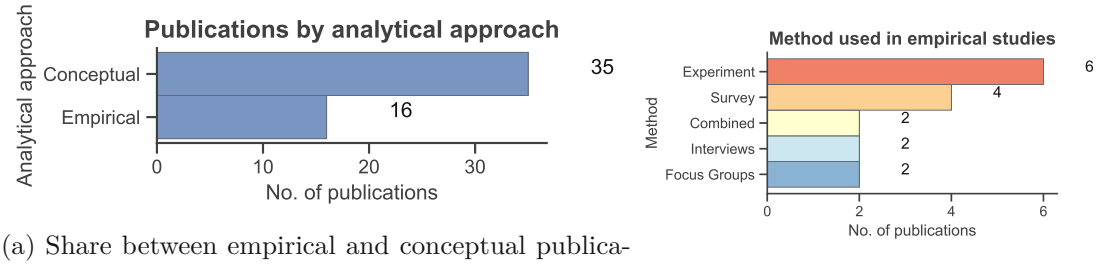
5.4 Lack of Empirical Knowledge

Lutz, Schöttler, et al. (2019) conclude that the body of empirical knowledge on the topic of privacy implications of social robots is thin and the sample sizes are small, with non representative results, and that those studies available mostly focus on informational privacy aspects. Among the major contributions to the topic, in this literature review it was found that most of the publications were conceptual (n=151) and significantly less were experimental (n=69), which can also be seen in Figure 5.1a. The distribution of the empirical methods used can be seen in Figure 5.1b. Of course, it can be argued that the novel nature of the topic is a contributing factor to the lack of empirical research on the topic. Nevertheless, empirical findings should be used to take into account the needs of the people to be cared for - because these factors can be underestimated or overestimated in a purely conceptual view. An example for a contradiction between the theory and the practice, would be the finding of Hoorn et al. (2015), that elderly participants of their experiment were only concerned about disclosing information, unless they were repeatedly told that they should be concerned. Although it does not reflect the exact same technology, experiments should be done with test subjects that reflect the various aspects of the preservation or invasion of privacy in multiple dimensions. This approach would also be in line with the flexible regulations regarding privacy preferred by Ishii (2019), Ienca and Eduard Fosch-Villaronga (2019) and Carnevale (2016), and might also help to deal with the unpredictable nature of AI technologies. With regard to **RQc**, it can be said that it is important to determine and define which technologies are suitable for care, and which are desired and accepted by caregivers, informal caregivers, relatives who may also have to operate them, and, of course, the people being cared for. In the course of such a development process, it can also be already thought about using only sensors which enhance privacy, e.g. LIDAR sensors instead of cameras. Only when technology is developed in collaboration with all involved parties, an actual assessment of the privacy impact is possible. Moreover, empirical knowledge could help to understand better the social and psychological dimensions of privacy in relation to care robots.

5.5 Taking Generational Change into Account

Care robots are still in a very experimental state, and it is likely it will remain like that for at least 20 to 30 years. Thus, the millennial generation – those in their 30s and 40s today –, will be the primary customer group of those devices when they are ready to enter the market. Keeping that in mind, it may be less of importance to put an extra focus on the design of graphical user interfaces for the elderly of today, but be aware that the future primary care robot users will be a generation that is highly tech-savvy, that grew up

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN



(a) Share between empirical and conceptual publications

(b) Method used in empirical studies

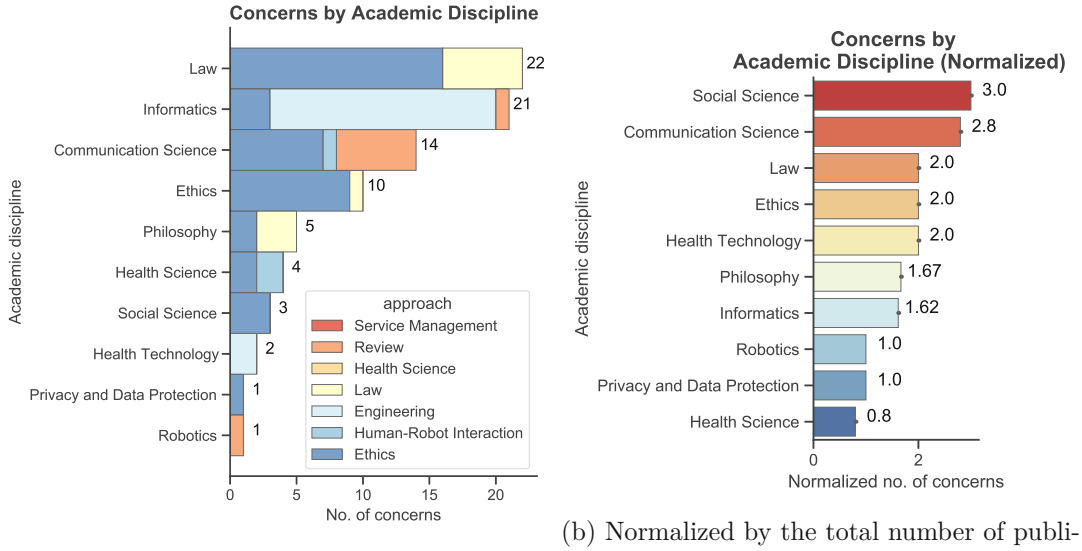
Figure 5.1: Analytical approach and methods of empirical studies (only major contributions)

using the internet and smartphones. While it is true that »interfaces should be designed to optimize older users' ability to authenticate, configure settings, and accomplish other security tasks without errors in a reasonable time« (Frik et al., 2019, p.31), roboticists of today should be aware that the average user of a care robot in the future is likely to be more tech-savvy than the average older adult of today. Whether the future older adults are more or less likely to be willing to share sensitive information via the internet, as they grew up using mobile devices and social media, is a matter of speculation and would need more investigation. For further research, it would be interesting to determine the attitudes of the younger generation of today, in order to learn about privacy perceptions for future technologies.

5.6 Engineer's Rationality?

Lutz and Tamò (2015) described a conflict between efficiency and effectivity, meaning that engineers would focus more on functionality while regulators would incorporate responsibility, such as the protection of privacy, into the development process. This is what they call the »engineer's rationality.« This would suggest that publications by authors from the academic disciplines of informatics or engineering, would have less concerns, and thus also propose less mitigation strategies for privacy violations, while authors from the discipline law should take those topics more frequently into account. In order to get to the bottom of this matter, the publications were analyzed for the number of mentions of concerns respectively mitigation strategies. In Figure 5.2a the number of concerns is shown listed by the different academic disciplines. If a concern is addressed in publication, it was counted once, but the same concerns appear multiple times in the total. In order to take into account that the number of different publications from the academic disciplines is different, the totals in the graph were normalized (see Figure 5.2b) with the number of publications which can be seen in Figure 4.1. Figure 5.3a shows the number of mitigation strategies mentioned, also only counted once per publication. In Figure 5.3b the number of mitigation strategies was normalized with the respective total count of publications of each academic discipline.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN



(a) Overall number of concerns

(b) Normalized by the total number of publications in each academic disciplines

Figure 5.2: Number of concerns discussed in the different academic disciplines (only major contributions)

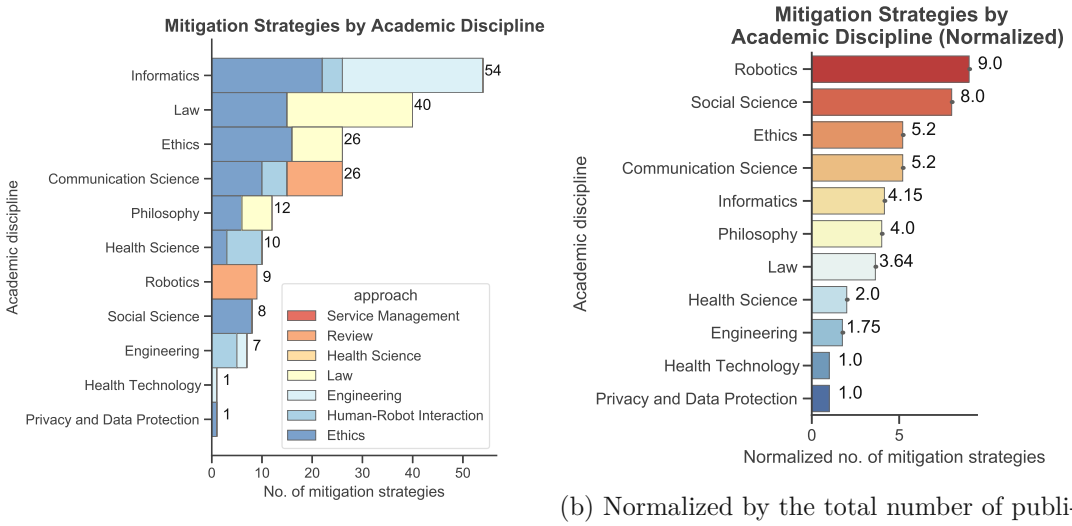
If analyzing at the normalized values in Figures 5.2a and 5.3a, there is no significant difference between the engineering and law disciplines regarding concerns regarding the preservation of privacy and the proposed number of mitigation strategies. As for this literature review only publications were included, which discuss the topic of privacy, the body of literature definitively has a high probability of dealing with privacy in a critical way. What can be said, is that in both categories, the number of overall concerns and overall mitigation strategies, law and informatics disciplines have the highest amount of mentions of the terms – this suggests that there is indeed a lively discourse on concerns and related mitigation strategies. Robotics and engineering on the other hand, seemingly have less concerns, while the publications from the academic approach robotics (n=1) included in the literature review propose a large number of mitigation strategies. In Figure 3.4a it can furthermore be seen that the majority of publications of the academic discipline of robotics in have only minor consideration of privacy aspects.

Nevertheless, to make a statement about the overall behavior of the »engineers rationality« with respect to privacy, other inclusion criteria would have to be chosen in the literature review, which do not analyze those works that specifically target privacy.

5.7 Proceed with Caution

Calo (2020) finds that neither law nor technology has prevent privacy harm effectively, and thus development of social robots should be proceeded careful; this assessment appears all the more important, as Lutz and Tamó-Larrieux (2020) point out that there

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN



(a) Overall number of mitigation strategies

(b) Normalized by the total number of publications in each academic disciplines

Figure 5.3: Number of mitigation strategies discussed in the different academic disciplines (only major contributions)

are currently only moderate concerns related to privacy impact of social robots among potential users. Unfortunately, often privacy in regards to data is disregarded, with the statement their data is not as valuable for profiteers (e.g., Frik et al., 2019). Huber and Camp (2017) found that older people value their key relationships more than their privacy, and would let relatives install any device in their home if it would make them feel better.

The violation of privacy is not a trivial offense, neither can and should it be reduced purely to a matter of personal well-being. The selling of psychological profiles of Facebook users by Cambridge Analytica,[20] was used by the Trump campaign to target advertisements and to support »Brexit Leave« campaigners; the scandal affected as many as 87 million users and it was discovered later that Facebook most likely knew about the leak but did not act immediately.[21] In a more recent scandal the Pegasus spyware was used to access iOS as well as Android mobile devices, which Amnesty International call a violation to human rights, as people around the world are unlawfully targeted, and also human rights activists were systematically targeted.[9] The New York summarize the concerns of privacy activists »[...] no smartphone user — even those using software like WhatsApp or Signal — is safe from governments and anyone else with the right cyber-surveillance tech.«[22] The unauthorized invasion of our privacy is to be seen very critically, even

[20] https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html, last accessed November 28, 2021

[21] https://www.businessinsider.com/cambridge-analytica-a-guide-to-the-trump-linked-data-firm-that-harvested-50-million-facebook-profiles-2018-3, last accessed November 28, 2021

[22] https://www.nytimes.com/2021/07/18/world/middleeast/israel-nso-pegasus-

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

if individual persons concerned think they have nothing to hide. The real impact on society, such as influencing political opinions, can be taken to extremes by social robots, since - unlike in the Cambridge Analytica scandal - the advertisements can not only be placed prominently in the Facebook feed, but could literally be in the living room of affected individuals. There is also no reason to believe that, if it is possible, humans will purposefully use robots in a malicious manner to physically attack other humans. Social engineering attacks, will be possible on a completely different level with a social robot at home, therefore awareness on the topic is urgently proposed.

On the other hand, there is good regulation in place at least in the EU, with the GDPR which is in force since May 2018 there is legally binding requirement to implement PbD, the right to be forgotten, data portability and transparency GDPR Eduard Fosch-Villaronga and Albo-Canals (2019). Moreover there are privacy activists, such as Max Schrems, who challenge the practices of data transfer from the EU to the United States, as there would be no protection against surveillance.[23] Also, the EU has guidelines regarding the development of trustworthy AI, recommending best practices to tackle many of the issues that were raised regarding AI in the literature review, such as data protection, quality and integrity of data, access to data, transparency, traceability and explainability.[19] These guidelines are hardly considered in the current view of privacy in care robots in relation to emerging technologies - however, the guidelines were also only recently published as a draft in 2018. In summary, there is reason to be cautious, but it will not be possible to avoid data breaches and to learn from them. This again speaks in favor of a flexible legislation based on clear, easily understandable principles, which, however, gives as few opportunities as possible to exploit loopholes.

In any case, future research should address the question of how aware future users of care robots are of the possibilities of privacy violations.

5.8 Other Issues that Need to be Addressed

The privacy paradox is not featured prominently, but could be a major problem which would require rethinking approaches related to the mitigation of privacy infringements. The Fair Information Practices (FIPs) (e.g., Gellman, 2019), are not often mentioned, although they are referred to by Lutz, Schöttler, et al. (2019), as an important approach to preserve privacy. Furthermore, most publications do not go into detail how certain guidelines, such as the Privacy by Design (PbD) approach or the concept of contextual integrity by Nissenbaum (2004) should actually be implemented in the robotic solution. The same applies to data protection, which is mentioned often but is not further specified how it should be achieved. Shape extraction as mentioned by Demiris et al. (2009) is an approach which should be further investigated, and might help with implementing PbD of robots.

spyware.html, last accessed November 28, 2021

[23] https://epic.org/documents/data-protection-commissioner-v-facebook-and-max-schrems-standard-contractual-clauses/, last accessed November 28, 2021

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

CHAPTER 6

Discussion and Conclusion

This thesis asks the question how the impact of care robots on privacy is currently negotiated in research. In the beginning, the need for care technology is discussed in the light of the upcoming demographic shift towards an ageing society, especially in the high-income countries around the world. Then, some technological solutions that resulted from research projects or are actually commercially in use are pointed out, to show the versatile application of the technologies. With that established knowledge, the research questions and hypotheses are formulated. Chapter 2 establishes the vocabulary and deepens the knowledge on the concepts used for the further analyses. The differentiation of care robot technologies is explained, and the different concepts for privacy are elaborated on. The most comprehensive and applicable concept of privacy for care robots, as defined by Burgoon (1982), was analysed and the four dimensions of privacy (i) physical privacy, (ii) social privacy, (iii) psychological privacy and (iv) informational privacy were described in detail. Moreover a short description of emerging technologies is provided, as those become more important in the development of robots and pose particular threats for privacy. The main parts of thesis are the following three chapters: the description of the method used for the literature review and an overview of the relevant literature (Chapter 3), followed by the qualitative review of the contents of the major contributions to the research question (Chapter 4), and finally a section that addresses open questions for the future (Chapter 5).

The performed method to gather the relevant literature was described in Chapter 3. The included body of literature was limited to the years 2010 to 2021. Meta-data for the records have been taken, to analyze the body of literature further. Out of 220 publications on the topic of care robots, 89 (40.5%) consider privacy only in a minor way. The analysis furthermore shows that most (20.9%) of the publications can be attributed to the academic dicipline of informatics followed by health science with 16.8%. Philosophy and ethics together, would have a share of 16.8%, thus this would be the second largest group of contributors to the discourse. The number of publications from the United

States, the United Kingdom and the Netherlands amount to nearly half (45.0%) of the records found in the literature review. Mostly high-income countries, which at the same time are affected the most of the projected demographic shift, are publishing on the topic of care robots. The publications are originating from different academic disciplines, approach the topic in manifold ways, and are published in a variety of journals around the world. This interdisciplinary character of the research topic of care robots can be emphasized.

In Chapter 4 a detailed review of the literature which was categorized as major contribution was performed. Additionally, coding was used to identify prevalent narratives and notions, as well as mitigation strategies to reduce privacy violations. The privacy dimensions mostly considered are informational privacy and physical privacy. Only a few publications also consider social and psychological aspects, and even point out their importance, but nevertheless also empirical studies found that the informational and physical aspects are what users seemingly care the most about. The privacy impact of care robots seems to be a concern for users, as well as researchers. Nakedness is something where users are especially sensitive – with contradicting views on the solution: Fernandes et al. (2016) suggest the robot can be the object causing the privacy infringement, while Hoorn et al. (2015) argues that a robot could be an alternative to a caregiver, which would be less of a privacy infringement for patients. Also, the context of why a robot needs to be recording and who has access to the recordings is perceived important by users – medical personnel enjoys high trust in this regard. In general, users are concerned about having control over their data, but also they emphasize that having a certain degree of control over the robot is important, e.g. the possibility to switch off some functions or the robot completely, or to define zones where the robot is not allowed to go.

Researchers argue privacy concerns could lead to low acceptance, and it is pointed out that the privacy risks robots pose are less obvious as with current technologies. Nevertheless, there is the notion that privacy is not considered enough in robotic developments, and that definitely it should be considered also during the design and not in retrospect. An aspect that is also discussed is whether medical information will be safe with third parties. Furthermore, privacy is seen as a concept which is culturally bound and develops over time along the technology – and also that privacy perceptions differ among users. The most prevalent conflicts are the conflict of privacy and safety, as well as privacy and autonomy. Regarding the former, the narratives are whether a robot should be allowed to intervene to protect a person, or if safety justifies surveillance. For the latter, the narrative is that users are wiling to trade some of their privacy for the experienced autonomy and independence, which allows them to stay at home longer. The most prevalent concern is surveillance, as well as access to sensitive information of the house, and losing the right to one's own data. Also being monitored by informal caregivers (family, relatives, etc.) was seen as problem; while conversely the family members also felt uncomfortable when monitoring their relatives without their knowledge. It was also pointed out that people will behave different when they are being monitored; and that not only the patient who eventually gave consent to the monitoring might be affected

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

by it, but unknowing bystanders. The misuse of the data is another concern and in this context emerging technologies seem to be acknowledged as a development which requires a lot attention due to their incomprehensible nature. There is no regulation yet that is ready for the challenges for privacy, although the GDPR is perceived as an important step. Nevertheless, next to the regulation's strengths (e.g. the right to be forgotten or transparency), it also has weaknesses when it comes to the applicability of those measures and emerging technologies Artificial Intelligence (AI) and machine learning.

The most noted mitigation strategies are transparency, informed consent, the Privacy by Design (PbD) approach and the »contextual integrity« concept by Nissenbaum (2004). Transparency is mentioned in terms that it needs to be clear who is processing data, what data is processed and why. Furthermore, it must also be transparent which sensory capabilities a robot has. Informed consent should be given in a »rolling« form, meaning that the consent is renewed now and then. This also included patients with declining cognitive capacities, so that the most recent decisions regarding privacy are preserved, and at some point a legal carer will have to take over the decision-making. On the other hand, authors point out that informed consent might become impossible if AI and machine learning algorithms are used. The PbD approach is frequently mentioned, as it would implement privacy already in the development of the care robots. In the approach the maximum degree of privacy is required as default, and developers are forced to be proactive and ensure transparency. It is also pointed out that such proactive development is required due to the GDPR. Collected data should be minimized to the absolute necessary – which at the same time is conflicting to big data analysis. Nevertheless, there is criticism that PbD could be to inflexible as a pre-programmed solution. The contextual integrity approach asks to apply privacy norms according to different contexts. Also, it is mentioned that the roles of people change, and it might be hard for a robot to distinguish whether it can bring up sensitive personal information in front of bystanders. Furthermore, the integrity of the data can be damaged, e.g. if it mistakenly collects data about other people than the patient. The potential of Artificial Intelligence (AI) and machine learning to be used effectively to protect privacy was also pointed out. Regulation will have a major role in terms of mitigating privacy violations. A possible development would be flexible regulation, based on foundations, that would develop over time along with the technology. Technological mitigation strategies are for example to give the ability to switch off the robot – partially or fully –, shape extraction, turn the camera away, express intent, or signal the recording either with an audio signal or visually. Furthermore, avoiding certain areas in the living space is perceived as privacy maximizing feature. Moreover simple technological implementations of PbD that were suggested, e.g. to mount sensors in specific heights so that they cannot identify people.

It was found that a large number of publications on care robots and related technologies only have minor considerations on their privacy impact. Out of 220 publications on the topic of care robots, 89 (40.5%) consider privacy only in a minor way. As can be seen in Figure 4.2, most of the publications analyzed focus on the informational privacy aspect. The implementation of the GDPR had an influence on the publications on care robots,

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek WIEN Your knowledge hub

as it is detailed in Section 4.4.5. After the implementation of the regulation, it is brought up frequently. The impact of emerging technologies on privacy issues are considered more often in recent publications, as found in Section 4.3.5. Emerging technologies are a part of discussion, gaining more interest over the last years as can be seen in Figure 4.4. Furthermore, it was found that despite large scale privacy violations in the recent years, the threat of manipulation of users is not considered frequently. The awareness for the possible social engineering attacks, and the scale that personal care robots could have seems not yet to have arrived in the discourse. Thus, this is suggested as a future research topic in Section 5.1.

There is a general consensus that the advantages of assisstive technologies, social and care robots outweigh the privacy risks that they pose. The EU's GDPR is a good starting point when it comes to the mandatory data protection impact assessment (DPIA), privacy by design, the right to be forgotten, the right to object and the right to know. But especially emerging technologies such as cloud computing, big data and machine and deep learning pose threats in terms of uncontrollable storing and processing of data. Not only is it hard to control the privacy harms caused by this forms of data mining, but if one would exercise the »right to be forgotten,« it could lead to inconsistencies in the data sets. In conclusion, the expected benefits of care technology, especially for the elderly, were found to outweigh the potential threats to privacy, while caution was urged for anticipatory development.

Research Questions To answer research question **RQ** ("How does current literature consider the impact on privacy by care robots, socially assistive robots or ambient assisted living technologies?"), it can be summarized that privacy is considered mostly from the informational and physical dimensions, thus the privacy impact and the related mitigation strategies are more focused on those aspects. Nevertheless, there are publications pointing out the social component of robots as especially challenging. **RQa** ("What, where and by whom has been published?") is discussed in Chapter 3 in detail. The publications are mostly from high-income countries, most notably the United States, the United Kingdom and the Netherlands. **RQb** ("How is privacy currently being negotiated in science?") is answered in Chapter 4. The views on the impact of care robots on privacy are versatile, there is a certain amount of caution, while the advantages are highlighted and thus, privacy needs to be considered in-depth while the development of care robots will proceed. **RQc** ("Which questions have to be addressed in the future?") is answered in Chapter 5, most notably is the demand for more insight into the impact on social and psychological privacy, as well as the need for further empirical research.

Discussion Some suggestions for further research were identified in Chapter 5, these include the using emerging technologies to actually enhance privacy, gathering more empirical knowledge on the user perceptions on privacy, as well as the possible impact it can have. Moreover, the dimensions of social and psychological privacy should be researched more, as they definitely will be of importance with the introduction of (social) care robots.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

APPENDIX A

Tables of the Literature Overview

A.1 Variables

Variable	Values	Description
year *Year of the publication.*	2009 – 2021	The year of the publication, although the initial search was limited between 2010 and 2021, some publications were referred to in other studies and thus included into the analysis. For publications that were published multiple times, the newer publication date was taken into account (e.g., Calo, 2020).
focus *The main focus of the publication.*	care robots robotics	Care robots are at the core of the publication. The publication contains aspects of privacy, which are related to robotics in general, but can also be applied to care robots.
	childcare robots	The core discussion is about childcare robots, which share many similarities to care robots for the elderly or disabled, and thus aspects of privacy are related.
	robot law	The core discussion is about law and regulation regarding robots in general, but aspects of it can be applied to care robots.
analytical_approach *What is the analytical approach to the publication?*	conceptual	Discussion of existing literature, conceptual works raising new questions or ideas.
	empirical	Research results were obtained by doing empirical research, such as interviews, experiments etc. If the publication also includes a literature review next to the empirical part, for the meta-analysis it is anyways classified as empirical.

Table A.1: Variables used as meta-data in the literature overview

Variable	Values	Description
method *The method used in the analytical approach.*	–	The value is empty if the work is purely conceptual.
	{literature, systematic, scoping, narrative, qualitative, descriptive, integrative} review	Applies for conceptual works. If not specified further, the review is labeled a »literature review«.
	{survey, focus groups, interviews, experiment}	Applies for empirical works and is usually specified in the publication.
	exploratory	Can be both, empirical or conceptual in nature. The label is given if authors specify their publication as such.
	combined	Applies for both, empirical and conceptual works, and is used if multiple analytical approaches are used in the publication.
contribution *Level of consideration of the privacy impact of care robots or contribution to the topic.*	minor consideration	Publications that mention the aspect of privacy in the context of care robots only briefly (e.g., Tzafestas, 2018).
	major consideration	Publications that review publications on the privacy impact of care robots thoroughly, e.g. by devoting an entire paragraph or section to the subject (e.g., Decker, 2012).
	minor contribution	Publications that add a new aspect, or further emphasize known aspects to the privacy impact of care robots were classified as a minor contribution. Such could be an empirical study, which is not solely about privacy impact of care robots, but where the outcomes include such aspects (e.g., Allouch and Van Velsen, 2020).
	major contribution	Publications that add major new aspects to the privacy impact of care robots. This could be sorely conceptual papers, but also reviews (e.g., Heuer, Schiering, and Reinhard Gerndt, 2017) which fill a research gap or empirical studies (e.g., Schomakers and Ziefle, 2019) that have the privacy aspects in the center of their research.
citation_count *How many times was the publication cited?*	0 – ∞	The number of times the publication has been cited is fetched from Google Scholar as of August 2021 and is equivalent to the value displayed as »cited by« in the database entries.
approach *How are the researchers of the study approaching the privacy impact of care robots?*	engineering	Researchers that are developing hardware or software for applications for care robots.
	ethics	The main contribution of the publications are ethical considerations – not limited to privacy aspects only.
	health science	The authors are approaching the topic from the perspective of care personnel, medical staff, physicians, nursing, etc.
	human-robot interaction	The publication's main contribution is the interaction between robots and humans, often those publications are empirical in nature.
	law	The study is mostly about regulation, policy and laws concerning the use of care robots.
	review	The publication has no clear overall approach to the topic, as it is a review covering multiple dimensions of care robots.
	service management	Authors are discussing the role of care robots by the value they create for society in terms of service, jobs or business opportunities.
journal *Where was published?*	*miscellaneous*	Name of the journal, book or conference proceedings where the publication has been published.

Table A.2: Variables used as meta-data in the literature overview (continued)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Variable	Values	Description
journal_field *Main topic covered in the journal.*	*miscellaneous*	Main research topic listed in the journal – can be also »interdisciplinary« or »multidisciplinary« if the focus of the journal is not clear.
peer_reviewed *Is the publication peer-reviewed?*	TRUE *or* FALSE	Whether the journal/publication is peer-reviewed or not. Book chapters are regarded as non peer-reviewed.
author *Who published?*	*miscellaneous*	Unique name of the first author of the publication. Other authors are not regarded – many publications are inter- or multidisciplinary as the topic of robotics is of such nature. Limiting to the first author simplifies the meta-analysis, however, the fact is not forgotten when interpreting the results.
institution *Which institution is the author publishing from?*	*miscellaneous*	The name of the academic, research or other institution that the first author belonged to at the time of the publication. If multiple institutions are given on publication, the first academic institution (e.g. a University) is considered, if there no academic institution, the first institution is taken.
discipline *Academic discipline of the institution of the first author.*	*miscellaneous*	In order to achieve a value on the meta-level, the academic discipline is grouped by the highest available information, e.g. the departments of computer sciences and the department of software engineering both belong to the faculty of informatics, so the academic discipline would be regarded as informatics.
country *Where is the institution?*	*miscellaneous*	The name of the country where the institution of the first publishing author is located.

Table A.3: Variables used as meta-data in the literature overview (continued)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

A.2 Results

Category	**Frequency** (percentage)
Publications	Included for meta-analysis: 220 (100.0)
Academic discipline (no. of publications > 2)	Informatics: 46 (20.9) Health science: 37 (16.8) Philosophy: 18 (8.2) Ethics: 19 (8.6) Law: 20 (9.1) Engineering: 13 (5.9) Communication Science: 12 (5.5) Robotics: 12 (5.5) Social Science: 9 (4.1) Psychological Medicine: 5 (2.3) Health technology: 4 (1.8) Marketing: 3 (1.4) Business Science: 3 (1.4)
General approach	Ethics: 81 (36.8) Human-Robot Interaction: 53 (24.1) Engineering: 29 (13.2) Law: 19 (8.6) Health Science: 17 (7.7) Review: 15 (6.8) Service Management: 6 (2.7)
Analytical approach	Conceptual: 151 (68.6) Empirical: 69 (31.4)
Country of first authors' institutions (no. of publications > 4)	United States: 38 (17.3) United Kingdom: 34 (15.5) Netherlands: 27 (12.3) Italy: 13 (5.9) Germany: 11 (5.0) Australia: 9 (4.1) New Zealand: 8 (3.6) Japan: 6 (2.7) Switzerland: 7 (3.2) Norway: 7 (3.2) Finland: 7 (3.2) Ireland: 7 (3.2) Belgium: 5 (2.3)

Table A.4: Summary of the results of the literature overview

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Category	Frequency (percentage)
First authors (no. of publications > 2)	Fosch-Villaronga: 7 (3.2) Vandemeulebroucke: 5 (2.3) Coeckelbergh: 4 (1.8) Lutz: 4 (1.8) Broadbent: 4 (1.8) Sharkey, A.: 4 (1.8) Sharkey, N.: 3 (1.4) Ienca: 3 (1.4) Felzmann: 3 (1.4) Van Wynsberghe: 3 (1.4) Royakkers: 3 (1.4)
Institutions of first authors (no. of publications > 4)	University of Twente: 8 (3.6) University of Sheffield: 8 (3.6) University of Auckland: 6 (2.7) Eindhoven University of Technology: 5 (2.3) University of Leuven: 5 (2.3) University of Washington: 5 (2.3) National University of Ireland: 5 (2.3) Indiana University Bloomington: 5 (2.3) Sant'Anna School of Advanced Studies: 5 (2.3)
Scholarly publication (no. of publications > 5)	International Journal of Social Robotics: 12 (5.5) Ethics and Information Technology: 9 (4.1) Science and Engineering Ethics: 6 (2.7) Journal of Medical Internet Research: 6 (2.7) International Conference on Social Robotics: 6 (2.7) International Conference on Human-Robot Interaction: 7 (3.2)

Table A.5: Summary of the results of the literature overview (continued)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

APPENDIX B

Tables of the Qualitative Analysis

B.1 Codebook

Concern	
Concern: Access	
Definition	A robot, or another health related technology, is used to access information inside a living space, which would otherwise be hidden. Such as a printout of bank information or other sensitive documents.
Example	»[...] participants highlighted that the ability to physically reach out into the world in an autonomous fashion enables robots to surveil individuals across places and gain access to personal rooms, which was impossible at this scale before.« (Eduard Fosch-Villaronga, Tamò-Larrieux, et al., 2018, p.8)
Occurrence	Calo (2011), Eduard Fosch-Villaronga, Tamò-Larrieux, et al. (2018), and A. Sharkey and N. Sharkey (2012)
Concern: Access lawful	
Definition	Access to information inside an otherwise private space by legal means (e.g. governments).
Example	»The government could lawfully gain access to robot sensory information—including real time audio and video—with sufficient process.« (Calo, 2011, p.941)
Occurrence	Calo (2011), Kaminski (2014), Novitzky et al. (2015), and Sedenberg et al. (2016)
Concern: Access unauthorized	
Definition	Access to information inside an otherwise private space by unauthrized means (e.g. hackers).
Example	»The home robot in particular presents a novel opportunity for government, private litigants, and hackers to access information about the interior of a living space.« (Calo, 2011, p.941)
Occurrence	Felzmann et al. (2016), Eduard Fosch-Villaronga, Tamò-Larrieux, et al. (2018), García-Soler et al. (2018), Ienca, Wangmo, et al. (2018), Jecker (2020), and Lutz, Schöttler, et al. (2019)
Concern: Control	
Definition	Gaining physical control over a care robot.
Example	»We were only able to control the Rovio and the Spykee using legitimate login credentials.« (Denning et al., 2009, p.108)
Occurrence	Calo (2011, 2020), Denning et al. (2009), Eduard Fosch-Villaronga, Tamò-Larrieux, et al. (2018), and Jecker (2020)

Table B.1: Codebook

Concern: Control lawful	
Definition	Gaining physical control over a care robot by legal means.
Example	»And, unlike a standard security or computer camera, law enforcement could move a robot around the interior of the home in pursuit of contraband.« (Calo, 2011, p.941)
Occurrence	Calo (2011, 2020) and Kaminski (2014)
Concern: Control unauthorized	
Definition	Gaining physical control over a care robot in an unauthorized manner.
Example	»The attacker uses the remote and repeater to issue commands to the RoboSapien from a distance. This allows him to control its movements, while the Rovio is maneu- vered to provide a view of the RoboSapien and the environment.« (Denning et al., 2009, p.111)
Occurrence	Denning et al. (2009), Eduard Fosch-Villaronga, Tamò-Larrieux, et al. (2018), García-Soler et al. (2018), and Lutz, Schöttler, et al. (2019)
Concern: Information disclosure	
Definition	Release of data to e.g. an unwanted third party.
Example	»When robots collect all this information that is directly related to the private sphere of the lives of its users, it may accidentally or intentionally disclose such information to a third party.« (Felzmann et al., 2016, p.283)
Occurrence	Felzmann et al. (2016), Ienca and Eduard Fosch-Villaronga (2019), and Jecker (2020)
Concern: Physical attack	
Definition	A care robot is used to launch a physical attack on a person.
Example	»The Rovio could be used to trip an elder with limited stability and mobility, particularly if the elder has impaired hearing and cannot notice the Rovio approaching.« (Denning et al., 2009, p.110)
Occurrence	Denning et al. (2009), Frik et al. (2019), Jecker (2020), and Simshaw et al. (2015)
Concern: Privacy paradox	
Definition	Concerns related to the privacy paradox, meaning that user are acting contrary to their believe in privacy protection.
Example	»Research on the privacy paradox has shown that in many scenarios users value privacy but are quick to give it up for short-term monetary or social rewards.« (Rueben et al., 2018, p.82)
Occurrence	Lutz, Schöttler, et al. (2019), Lutz and Tamò (2015), Lutz and Tamó-Larrieux (2020), and Rueben et al. (2018)
Concern: Social meaning	
Definition	Robots might cause people to interact with them freely and openly reveal sensitive information.
Example	»Yet there is another sense in which robots and artificial intelligence implicate privacy that is not as easy to redress: these technologies tend to possess social meaning.« (Calo, 2011, p.941)
Occurrence	Kaminski (2014), Lutz, Schöttler, et al. (2019), Lutz and Tamò (2015), and Lutz and Tamó-Larrieux (2020)
Concern: Surveillance	
Definition	Using robotic technology to surveil (or to monitor) people.
Example	»There are many ways to address the privacy issues of greater surveillance and access.« (Calo, 2011, p.941)
Occurrence	Armbrust et al. (2011), Calo (2011, 2020), Demiris et al. (2009), Denning et al. (2009), Draper and Sorell (2017), Eduard Fosch-Villaronga, Tamò-Larrieux, et al. (2018), Frik et al. (2019), Lutz, Schöttler, et al. (2019), Lutz and Tamò (2015), Schomakers and Ziefle (2019), Sedenberg et al. (2016), A. Sharkey and N. Sharkey (2012), Thorstensen (2018), and Townsend et al. (2011)

Table B.2: Codebook (continued)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Conflict	
Conflict: Privacy v autonomy	
Example	»Older adults are willing to trade privacy (by accepting a monitoring technology), for autonomy.« (Townsend et al., 2011, p.4749)
Occurrence	Van Heek et al. (2017), Ienca and Eduard Fosch-Villaronga (2019), and Townsend et al. (2011)
Conflict: Privacy v beneficence	
Example	»For example, the doctor of a patient with mild dementia may gain valuable treatment-related information from monitoring the patient's everyday behavioral habits even without the patient's consent. However, this unauthorized monitoring might represent an intrusion into that patient's privacy. In these situations, the protection of the patient's informational privacy might conflict with the physician's duty of beneficence and following each principle would lead to different courses of action.« (Ienca and Eduard Fosch-Villaronga, 2019, p.4)
Occurrence	Ienca and Eduard Fosch-Villaronga (2019), Lutz, Schöttler, et al. (2019), Lutz and Tamó-Larrieux (2020), and Townsend et al. (2011)
Conflict: Privacy v safety	
Definition	Should a robot be always in the same room as person to help in case of emergency, or should the robot avoid the person to grant privacy?
Example	»Obviously, violating the right to privacy in this way could be appropriate in some circumstances, such as those of intensive care. However, for those in partial or home care, it could be a severe intrusion on their privacy to monitor them taking a shower or using the bathroom, for example.« (N. Sharkey and A. Sharkey, 2011, p.269)
Occurrence	Armbrust et al. (2011), Frik et al. (2019), Ienca and Eduard Fosch-Villaronga (2019), Schafer and Edwards (2017), N. Sharkey and A. Sharkey (2011), and Theoharidou et al. (2017)
Definition	
Definition: Privacy	
Definition	The publication provided a general definition of privacy.
Occurrence	Armbrust et al. (2011), Carnevale (2016), Felzmann et al. (2016), and Ienca and Eduard Fosch-Villaronga (2019)
Definition: Privacy Brandeis	
Definition	Defining privacy as »the right of the individual to be let alone« (Brandeis and Warren, 1890, p.4).
Example	»One of privacy's central roles in society is arguably to help create and safeguard moments when people can be alone.« (Calo, 2011, p.941)
Occurrence	Armbrust et al. (2011), Calo (2011), Ienca and Eduard Fosch-Villaronga (2019), Ishii (2019), Lutz and Tamò (2016), Lutz and Tamó-Larrieux (2020), Reinhardt et al. (2021), and Yusif et al. (2016)
Definition: Privacy Burgoon	
Definition	Defining privacy in the four dimension proposed by Burgoon (1982).
Occurrence	Lutz, Schöttler, et al. (2019), Lutz and Tamò (2016), Rueben et al. (2018), and Schomakers and Ziefle (2019)
Definition: Privacy Westin	
Definition	Defining privacy by referring to Westin (1968).
Occurrence	Ienca and Eduard Fosch-Villaronga (2019), Lutz, Schöttler, et al. (2019), Lutz and Tamò (2016), Lutz and Tamó-Larrieux (2020), Reinhardt et al. (2021), and Sedenberg et al. (2016)

Table B.3: Codebook (continued)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Dimension	
Dimension: Informational	
Definition	Discussing the informational dimension of privacy.
Example	»The identified publications differ in their understanding of privacy. The majority are concerned with informational privacy.« (Lutz, Schöttler, et al., 2019, p.418)
Occurrence	Blake (2019), Carnevale (2016), Demiris et al. (2009), Fernandes et al. (2016), Fiske et al. (2019), Eduard Fosch-Villaronga, Tamò-Larrieux, et al. (2018), Frik et al. (2019), Heuer, Schiering, and Reinhard Gerndt (2017), Ienca and Eduard Fosch-Villaronga (2019), Ienca, Wangmo, et al. (2018), Ishii (2019), Kaminski (2014), Lutz, Schöttler, et al. (2019), Lutz and Tamò (2015, 2016), Lutz and Tamó-Larrieux (2020), Pagallo (2013), Reinhardt et al. (2021), Schomakers and Ziefle (2019), Sedenberg et al. (2016), Simshaw et al. (2015), Theoharidou et al. (2017), Thorstensen (2018), Vallverdú and Casacuberta (2015), and Yusif et al. (2016)
Dimension: Informational only	
Definition	Stating that for care robots only the informational dimension of privacy is relevant or leave out other dimensions than informational completely.
Example	»Among them, information privacy is the most relevant to the acceptance of robot technology.« (Alaiad and Zhou, 2014, p.829)
Occurrence	Bartoletti (2019), Felzmann et al. (2016), and Vallverdú and Casacuberta (2015)
Dimension: Physical	
Definition	Discussing the physical dimension of privacy.
Example	»The dimension of physical privacy is affected by the physical nature and mobility of social robots, while social robots' data collection and processing capacities affect users' informational privacy.« (Lutz, Schöttler, et al., 2019, p.416)
Occurrence	Blake (2019), Carnevale (2016), Demiris et al. (2009), Fernandes et al. (2016), Fiske et al. (2019), Eduard Fosch-Villaronga, Tamò-Larrieux, et al. (2018), Frik et al. (2019), Ienca and Eduard Fosch-Villaronga (2019), Ienca, Wangmo, et al. (2018), Lutz, Schöttler, et al. (2019), Lutz and Tamò (2016), Lutz and Tamó-Larrieux (2020), Reinhardt et al. (2021), Schomakers and Ziefle (2019), Sedenberg et al. (2016), N. Sharkey and A. Sharkey (2011), and Yusif et al. (2016)
Dimension: Psychological	
Definition	Discussing the psychological dimension of privacy.
Example	»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.« (Lutz, Schöttler, et al., 2019, p.416)
Occurrence	Fiske et al. (2019), Eduard Fosch-Villaronga and Albo-Canals (2019), Frik et al. (2019), Heuer, Schiering, and Reinhard Gerndt (2017), Lutz, Schöttler, et al. (2019), Lutz and Tamò (2016), Reinhardt et al. (2021), Schomakers and Ziefle (2019), and Sedenberg et al. (2016)
Dimension: Social	
Definition	Discussing the social dimension of privacy.
Example	»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.« (Lutz, Schöttler, et al., 2019, p.416)
Occurrence	Eduard Fosch-Villaronga and Albo-Canals (2019), Heuer, Schiering, and Reinhard Gerndt (2017), Lutz, Schöttler, et al. (2019), Lutz and Tamò (2016), Reinhardt et al. (2021), and Schomakers and Ziefle (2019)
Emerging technology	
Emerging technology: Artificial intelligence	
Definition	Privacy aspects related to Artificial Intelligence (AI).
Example	»Research in embodied artificial intelligence (AI) has increasing clinical relevance for therapeutic applications in mental health services.« (Fiske et al., 2019, p.1)
Occurrence	Felzmann et al. (2016), Fiske et al. (2019), Ienca, Wangmo, et al. (2018), Ishii (2019), Li and T. Zhang (2017), Lutz, Schöttler, et al. (2019), Lutz and Tamò (2015), Lutz and Tamó-Larrieux (2020), Simshaw et al. (2015), Thorstensen (2018), and Vallverdú and Casacuberta (2015)
Emerging technology: Big data	
Definition	Privacy aspects related to big data.
Example	»However, while big data has a huge potential to create significant value, it also contributes to qualitatively new concerns with regard to the use of personal information.« (Felzmann et al., 2016, p.280)
Occurrence	Felzmann et al. (2016), Ishii (2019), Kaminski (2014), Lutz, Schöttler, et al. (2019), Lutz and Tamò (2015, 2016), Sedenberg et al. (2016), Simshaw et al. (2015), and Vallverdú and Casacuberta (2015)

Table B.4: Codebook (continued)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Emerging technology: Cloud computing	
Definition	Privacy aspects related to cloud computing.
Example	»Although cloud robotics allows robots to benefit from the powerful computational, storage, and communications resources of cloud computing, it also brings challenges regarding security and privacy.« (Felzmann et al., 2016, p.282)
Occurrence	Felzmann et al. (2016), Eduard Fosch-Villaronga and Albo-Canals (2019), Li and T. Zhang (2017), Lutz, Schöttler, et al. (2019), Lutz and Tamò (2016), Pagallo (2013), and Simshaw et al. (2015)
Emerging technology: Cloud storage	
Definition	Privacy aspects related to cloud storage.
Example	»Consequently, by collecting information in open or public environments and, moreover, bringing such environmental information to cloud servers, robots-in-the-cloud can severely impinge on current data protection, since these machines may replicate and spread all the data they collect without any human "in the loop."« (Pagallo, 2013, p.502)
Occurrence	Kaminski (2014), Lutz, Schöttler, et al. (2019), Pagallo (2013), Sedenberg et al. (2016), Simshaw et al. (2015), and Theoharidou et al. (2017)
Emerging technology: Internet of things	
Definition	Privacy aspects related to the Internet of Things (IoT), sometimes also referred to in the context of ubiquitous computing systems.
Example	»Though the principles discussed here may apply more broadly to any robotic device or even other ubiquitous computing objects within the home (or perhaps in other sensitive settings), therapeutic robots provide a particularly salient ve- hicle for highlighting the opportunities and risks for users and researchers, and the need for guidance at this critical moment of commercial readiness.« (Sedenberg et al., 2016, p.4)
Occurrence	Felzmann et al. (2016), Ishii (2019), Lutz and Tamò (2015, 2016), Lutz and Tamó-Larrieux (2020), Pagallo (2013), Schulz et al. (2018), Sedenberg et al. (2016), Simshaw et al. (2015), Theoharidou et al. (2017), and G. Yang et al. (2018)
Emerging technology: Machine learning	
Definition	Privacy aspects related to machine learning.
Example	»The unpredictability arising from the AI machine learning function poses further difficulties, which have only been partially addressed by legal frameworks in the aforementioned jurisdictions.« (Ishii, 2019, p.509)
Occurrence	Ishii (2019), Li and T. Zhang (2017), Schafer and Edwards (2017), Schulz et al. (2018), Sedenberg et al. (2016), Simshaw et al. (2015), and Thorstensen (2018)
Issue	
Issue: Trust	
Definition	An issue related to robots is trust, which is often brought up as a requirement for acceptance.
Example	»The contribution of this study is in its exploration of end-user willingness to trust known AI decisions and unwillingness to trust unknown AI decisions. « (Poulsen and Burmeister, 2019, p.1)
Occurrence	Fernandes et al. (2016), Poulsen and Burmeister (2019), Rueben et al. (2018), and Schulz et al. (2018)
Mitigation strategy	
Mitigation strategy: Anonymizing data	
Definition	Preserve privacy by anonymizing data in any case.
Example	»[...] software tools for encryption and anonymizing data enable users to set limits to how information is shared beyond the robot-human encounter.« (Jecker, 2020, p.6)
Occurrence	Jecker (2020), Lutz, Schöttler, et al. (2019), and Theoharidou et al. (2017)
Mitigation strategy: Contextual integrity	
Definition	Analyzing contexts for applying different norms of privacy, according to the principle of contextual integrity by Nissenbaum (2004).
Example	»Contextual analysis invites a nuanced regulatory framework tailored to diverse social domains. Privacy controls appropriate in the context of a pandemic will reasonably differ from those appropriate outside pandemic settings, because human-robot relationships will be more isolated from human social life, making them both more vulnerable to abuse and more integral to health.« (Jecker, 2020, p.6)
Occurrence	Ishii (2019), Jecker (2020), Kaminski (2014), Lutz, Schöttler, et al. (2019), Lutz and Tamò (2015, 2016), Reinhardt et al. (2021), Rueben et al. (2018), Schomakers and Ziefle (2019), Sedenberg et al. (2016), A. Sharkey and N. Sharkey (2012), and N. Sharkey and A. Sharkey (2011)

Table B.5: Codebook (continued)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Mitigation strategy: Control over data	
Definition	Giving the user control over the data.
Example	»Allowing users and others affected by the collection and use of personal information sufficient transparency and control is a further challenge that needs to be met.« (Felzmann et al., 2016, p.285)
Occurrence	Felzmann et al. (2016), Eduard Fosch-Villaronga and Roig (2017), Heuer, Schiering, and Reinhard Gerndt (2017), Ishii (2019), Schomakers and Ziefle (2019), Sedenberg et al. (2016), and Theoharidou et al. (2017)
Mitigation strategy: Data protection impact assessment	
Definition	Peforming a data protection impact assessment (DPIA) to mitigate privacy violations.
Example	»Still, the only binding requirement is to conduct a data protection impact assessment, an obligation laid down in the General Data Protection Regulation (Art. 35 of the GDPR).« (Eduard Fosch-Villaronga and Albo-Canals, 2019, p.86)
Occurrence	Eduard Fosch-Villaronga and Albo-Canals (2019), Eduard Fosch-Villaronga and Roig (2017), and Ienca and Eduard Fosch-Villaronga (2019)
Mitigation strategy: Expressing intent	
Definition	The robot expresses the intention of action to the users.
Example	»They are (i) the gaze of the robot, (ii) the distance between the robot and a user, and (iii) clarity in expressing intent of the robot.« (D. Yang et al., 2021, p.1)
Occurrence	A. Sharkey and N. Sharkey (2012), N. Sharkey and A. Sharkey (2011), and D. Yang et al. (2021)
Mitigation strategy: Informed consent	
Definition	Propsong informed consent as a mitigation strategy for privacy infringements.
Example	»If elements like informed consent as discussed below are incorporated into the initial design and deployment of therapeutic robots, private companies and users will benefit from researcher access aimed at improving therapeutic outcomes.« (Sedenberg et al., 2016, p.12)
Occurrence	Blake (2019), Felzmann et al. (2016), Frik et al. (2019), Ienca and Eduard Fosch-Villaronga (2019), Ienca, Wangmo, et al. (2018), Ishii (2019), Lutz, Schöttler, et al. (2019), Lutz and Tamò (2015), Novitzky et al. (2015), Reinhardt et al. (2021), Sedenberg et al. (2016), A. Sharkey and N. Sharkey (2012), Theoharidou et al. (2017), and Thorstensen (2018)
Mitigation strategy: Privacy by default	
Definition	Privacy by default, is often also mentioned in connection with privacy by design. It requires that the default settings are set to be privacy preserving in the most possible way.
Example	»Privacy by Design and Privacy by Default are considered to be the key solutions against the risks posed by AI robots.« (Ishii, 2019, p.516)
Occurrence	Ishii (2019), Lutz, Schöttler, et al. (2019), and Thorstensen (2018)
Mitigation strategy: Privacy by design	
Definition	Privacy by design as a propose mitigation strategy; privacy should be considered in the design process of a robot already.
Example	»According to good data protection practice, it will need to be ensured that data recorded and especially data stored longer term is not excessive and that data processing and storage options either minimise data usage or have significant advantages over less data intensive alternatives. This principled reduction of data storage is also a core tenet of privacy by design.« (Felzmann et al., 2016, p.283)
Occurrence	Felzmann et al. (2016), Eduard Fosch-Villaronga and Albo-Canals (2019), Eduard Fosch-Villaronga, Tamò-Larrieux, et al. (2018), Huber and Camp (2017), Ienca and Eduard Fosch-Villaronga (2019), Ienca, Wangmo, et al. (2018), Ishii (2019), Jecker (2020), Lutz and Tamò (2015), Novitzky et al. (2015), Pagallo (2013), Rueben et al. (2018), Schulz et al. (2018), and Simshaw et al. (2015)
Mitigation strategy: Privacy enhancing robots	
Definition	Robots which use various technological solutions to enhance privacy.
Example	»To protect the sensitive information at the beginning of data collection, we implemented a mechanism for a social robot to detect embarrassing situations and convert privacy information into non-sensitive information.« (G. Yang et al., 2018, p.23)
Occurrence	Calo (2020), Sedenberg et al. (2016), and G. Yang et al. (2018)

Table B.6: Codebook (continued)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Mitigation strategy: Privacy impact assessment	
Definition	Peforming a privacy impact assessment (PIA) to mitigate privacy violations.
Example	»ISO/IEC 29134:2017 is one of the only documents that establish some guidelines for conducting a privacy impact assessment.« (Eduard Fosch-Villaronga and Albo-Canals, 2019, p.86)
Occurrence	Eduard Fosch-Villaronga and Albo-Canals (2019), Eduard Fosch-Villaronga and Roig (2017), Ishii (2019), and Lutz and Tamò (2015)
Mitigation strategy: Regulation	
Definition	Mitigation of privacy violations by regulation or law in general.
Example	»Techno-regulation means many things. Firstly, facing the con-rete risks concerning a distorted and defected relationship between humans and technological devices and applications.« (Carnevale, 2016, p.145)
Occurrence	Blake (2019), Calo (2020), Carnevale (2016), Fiske et al. (2019), and Ienca and Eduard Fosch-Villaronga (2019)
Mitigation strategy: Regulation Fourth Amendment	
Definition	Regulation which referes the the U.S. fourth amendment.
Occurrence	Ienca and Eduard Fosch-Villaronga (2019), Ishii (2019), Kaminski (2014), and Sedenberg et al. (2016)
Mitigation strategy: Regulation GDPR	
Definition	Mitigation by applying the General Data Protection Regulation (GDPR) of the EU.
Example	»This is extremely important, because the legal domain in data protection matters is worried about the awareness of the collected data, informed consent, legitimate purpose and all the new rights coming with the GDPR implementation: data portability, right to be forgotten or privacy-by-design.« (Eduard Fosch-Villaronga and Roig, 2017, p.512)
Occurrence	Eduard Fosch-Villaronga and Albo-Canals (2019), Eduard Fosch-Villaronga and Roig (2017), Eduard Fosch-Villaronga, Tamò-Larrieux, et al. (2018), Ienca and Eduard Fosch-Villaronga (2019), Ishii (2019), Lutz, Schöttler, et al. (2019), Rueben et al. (2018), and Thorstensen (2018)
Mitigation strategy: Right to be forgotten	
Definition	Mitigation by the right to be forgotten.
Example	»This is extremely important, because the legal domain in data protection matters is worried about the awareness of the collected data, informed consent, legitimate purpose and all the new rights coming with the GDPR implementation: data portability, right to be forgotten or privacy-by-design.« (Eduard Fosch-Villaronga and Roig, 2017, p.512)
Occurrence	Eduard Fosch-Villaronga and Albo-Canals (2019), Eduard Fosch-Villaronga and Roig (2017), Ienca and Eduard Fosch-Villaronga (2019), Rueben et al. (2018), and Schulz et al. (2018)
Mitigation strategy: Security by design	
Definition	Implementation of security by design to mitigate privacy violations.
Example	»However, with security by design being difficult to achieve, measures for securing sensitive (e.g. behavioral, personal or physiological) information should be implemented not only at the level of product development but also of individual use and regulation.« (Ienca, Wangmo, et al., 2018, p.1048)
Occurrence	Ienca, Wangmo, et al. (2018), Novitzky et al. (2015), and Simshaw et al. (2015)
Mitigation strategy: Shape extraction	
Definition	Mitigation privacy infringments by extracting shapes of persons from the video.
Example	»The level of shape extraction that erases identifying features addresses privacy concerns and increases confidence in users that video-based monitoring can be useful and appropriate.« (Demiris et al., 2009, p.47)
Occurrence	Demiris et al. (2009), Novitzky et al. (2015), Rueben et al. (2018), and Schulz et al. (2018)

Table B.7: Codebook (continued)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Mitigation strategy: Signal by audio	
Definition	Make the user aware that e.g. the robot is recording by making a noise, or talking to the user.
Example	»For instance, devices should always make image capture clear through the use of a light or sound, and be designed to remind the users that recording is still active if a camera detects flesh more flesh tones (implying someone might be accidentally naked in front of the camera) or if the microphone detects arguing (indicating a sensitive conversation not relevant to the therapeutic application may be occurring).« (Sedenberg et al., 2016, p.17)
Occurrence	Lutz, Schöttler, et al. (2019), Schafer and Edwards (2017), Schulz et al. (2018), Sedenberg et al. (2016), A. Sharkey and N. Sharkey (2012), and D. Yang et al. (2021)
Mitigation strategy: Signal visually	
Definition	Making the user aware that e.g. the robot is recording by showing a visual signal, e.g. a blinking light.
Example	»For instance, devices should always make image capture clear through the use of a light or sound, and be designed to remind the users that recording is still active if a camera detects flesh more flesh tones (implying someone might be accidentally naked in front of the camera) or if the microphone detects arguing (indicating a sensitive conversation not relevant to the therapeutic application may be occurring).« (Sedenberg et al., 2016, p.17)
Occurrence	Lutz, Schöttler, et al. (2019), Schafer and Edwards (2017), Schulz et al. (2018), Sedenberg et al. (2016), A. Sharkey and N. Sharkey (2012), N. Sharkey and A. Sharkey (2011), and D. Yang et al. (2021)
Mitigation strategy: Switch off	
Definition	Ability to switch off the whole robot in order to avoid monitoring.
Example	»In the interest of users' autonomy and privacy, it is desirable for persons to have the option of switching off some of Mario's functions (or switching off the robot altogether), at least temporarily, unless doing so would bring significant risks.« (Felzmann et al., 2016, p.284)
Occurrence	Felzmann et al. (2016), Heuer, Schiering, and Reinhard Gerndt (2017), Lutz, Schöttler, et al. (2019), and Schomakers and Ziefle (2019)
Mitigation strategy: Transparency	
Definition	Transparency related to how data is processed and stored, but also being transparent about sensory capacities of a robot, e.g. by designing in a way that does not hide sensor capacities on purpose.
Example	»Allowing users and others affected by the collection and use of personal information sufficient transparency and control is a further challenge that needs to be met.« (Felzmann et al., 2016, p.285)
Occurrence	Felzmann et al. (2016), Eduard Fosch-Villaronga and Albo-Canals (2019), Eduard Fosch-Villaronga and Roig (2017), García-Soler et al. (2018), Heuer, Schiering, and Reinhard Gerndt (2017), Huber and Camp (2017), Ienca and Eduard Fosch-Villaronga (2019), Lutz and Tamò (2015), Poulsen and Burmeister (2019), Reinhardt et al. (2021), Rueben et al. (2018), Schafer and Edwards (2017), Sedenberg et al. (2016), Theoharidou et al. (2017), and D. Yang et al. (2021)
Mitigation strategy: Turn camera away	
Definition	Turning the camera of a robot away in order to prevent privacy sensitive siutations for users.
Example	»In our project, when a person is beginning to take off his or her clothes to go to sleep or to take a shower, the robot will turn away its camera to avoid capturing videos or images of the naked or partially naked person.« (Fernandes et al., 2016, p.727)
Occurrence	Fernandes et al. (2016), Rueben et al. (2018), and G. Yang et al. (2018)
	Privacy
Privacy: Contextual	
Definition	The view that privacy should be seen in context. Often used in combination with the contextual integrity approach by Nissenbaum (2004).
Example	»Privacy is not an absolute right but contextual, and intrusion of the private sphere is sometimes warranted. The interests of all parties involved have to be balanced.« (Carnevale, 2016, p.149)
Occurrence	Carnevale (2016), Ishii (2019), Kaminski (2014), Lutz, Schöttler, et al. (2019), Lutz and Tamò (2015, 2016), Pagallo (2013), Reinhardt et al. (2021), Rueben et al. (2018), Schomakers and Ziefle (2019), A. Sharkey and N. Sharkey (2012), and N. Sharkey and A. Sharkey (2011)
Privacy: Developing along technology	
Definition	The understanding of privacy and it's norms, and thus the resulting regulation, will be developed along the technological development.
Example	»Summing up, techno-regulation is surely important in order to provide legal norms to guide the technological development, but also to choose those political and ethical principles that will guide the technology in a determined direction, and not in another. « (Carnevale, 2016, p.145)
Occurrence	Bartoletti (2019), Carnevale (2016), and Novitzky et al. (2015)

Table B.8: Codebook (continued)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Robot effect	
Robot effect: Privacy enhancing behavior	
Definition	Whether the presence of a robot, monitoring or AI powered device triggers privacy enhancing behaviors (PEBs) of subjects.
Example	»Overall we found that older adults in each of the three monitoring conditions engaged in PEBs.« (Caine et al., 2012, p.348)
Occurrence	Caine et al. (2012), Wu et al. (2021), and G. Yang et al. (2018)

Safety	
Safety	
Definition	General aspects related to safety.
Example	»It will improve the situation of an elderly person, by offering attention, providing safety and still maintaining privacy.« (Armbrust et al., 2011, p.1)
Occurrence	Armbrust et al. (2011), Denning et al. (2009), Van Heek et al. (2017), Ienca and Eduard Fosch-Villaronga (2019), Novitzky et al. (2015), N. Sharkey and A. Sharkey (2011), and Simshaw et al. (2015)

Security	
Security	
Definition	General aspects related to security.
Example	»Of course, access to the robot should only be granted to authorised personnel, such as care-givers and relatives – a crucial requirement with respect to privacy and security of the elderly person.« (Armbrust et al., 2011, p.4)
Occurrence	Armbrust et al. (2011), Denning et al. (2009), Ienca and Eduard Fosch-Villaronga (2019), Ienca, Wangmo, et al. (2018), Lutz and Tamò (2016), Novitzky et al. (2015), and Wu et al. (2021)

Value	
Value: Ageing at home	
Definition	The value robots create, that enable older adults to stay independent longer, thus to age at home.
Example	»This could result in the elderly being able to stay out of institutional care for longer.« (N. Sharkey and A. Sharkey, 2011, p.268)
Occurrence	Schomakers and Ziefle (2019), A. Sharkey and N. Sharkey (2012), and N. Sharkey and A. Sharkey (2011)
Value: Autonomy	
Definition	The value of autonomy that robots create.
Example	»Having a robot pet may also give elders an increased feeling of control and autonomy.« (N. Sharkey and A. Sharkey, 2011, p.277)
Occurrence	Eduard Fosch-Villaronga, Tamò-Larrieux, et al. (2018), Van Heek et al. (2017), A. Sharkey and N. Sharkey (2012), and N. Sharkey and A. Sharkey (2011)
Value: Control	
Definition	Users value having control over their data, and also their physical environment, e.g. having the control to switch off a robot.
Example	»Such robots could make elderly people feel that they had even less control over their lives than when they are dependent on human nursing care.« (A. Sharkey and N. Sharkey, 2012, p.30)
Occurrence	Van Heek et al. (2017), N. Sharkey and A. Sharkey (2011), and Wu et al. (2021)

Table B.9: Codebook (continued)

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

List of Figures

1.1 Projected population developments of the EU-27 between 2001-2050 . . . 2

2.1 Concept of an Ambient Assisted Living (AAL) system by the GAIA-X project 8
2.2 Three examples of care robots with different approaches 10
2.3 Integrated solution for wearable health technologies by Technosoft Solutions 11

3.1 Method of the literature review 20
3.2 Publications by level of contribution 24
3.3 Number of publications per year (2010–2020) 25
3.4 Number of publications per academic discipline 26
3.5 Publications by country of the institution of the first author 27
3.6 First authors with two or more publications 28
3.7 Publications by institutions of first authors (more than two publications) 29
3.8 Analytical approach and methods of empirical studies 29
3.9 Publications by journals (more than 2 publications) 30
3.10 Publications by journal field (more than 2 publications) 30

4.1 All major contributions by academic discipline 32
4.2 Dimensions of privacy discussed in literature 33
4.3 Discussed concerns posed by care robots 43
4.4 No. of publications that consider emerging technologies 52
4.5 Mitigation strategies discussed in literature 54
4.6 No. of publications that consider the GDPR 64

5.1 Analytical approach and methods of empirical studies (only major contributions) 72
5.2 Number of concerns discussed in the different academic disciplines (only major contributions) 73
5.3 Number of mitigation strategies discussed in the different academic disciplines (only major contributions) 74

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

List of Tables

3.1 Database search settings 21
3.2 Database search terms and results 21
3.3 Criteria for the inclusion for the screening 21
3.4 Records excluded, with reasons 22

A.1 Variables used as meta-data in the literature overview 81
A.2 Variables used as meta-data in the literature overview (continued) 82
A.3 Variables used as meta-data in the literature overview (continued) 83
A.4 Summary of the results of the literature overview 84
A.5 Summary of the results of the literature overview (continued) 85

B.1 Codebook 87
B.2 Codebook (continued) 88
B.3 Codebook (continued) 89
B.4 Codebook (continued) 90
B.5 Codebook (continued) 91
B.6 Codebook (continued) 92
B.7 Codebook (continued) 93
B.8 Codebook (continued) 94
B.9 Codebook (continued) 95

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU WIEN Bibliothek Your knowledge hub

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.

Acronyms

AAL Ambient Assisted Living. vii, ix, 7–9, 38, 40–42, 44, 47, 48, 52, 53, 57, 59, 64, 97

AI Artificial Intelligence. ix, 17, 42, 48, 49, 51, 53, 58, 62–64, 70, 71, 75, 79

AI HLEG High-Level Expert Group on Artificial Intelligence. 48

CRIA care robot impact assessment. 63

DPIA data protection impact assessment. 59, 80, 92

ECHR European Convention on Human Rights. 12, 13, 16, 43

EIA environment impact assessment. 59

FDA U.S. Food and Drug Administration. 63

FIP Fair Information Practice. 52, 60, 62, 75

FTC U.S. Federal Trade Commission. 63

GDPR General Data Protection Regulation. 24, 25, 33, 41, 47, 51, 52, 58, 59, 62–65, 75, 79, 80, 93

HHR home healthcare robot. 36, 43

HIPAA Health Insurance Portability and Accountability Act. 63

HRI human-robot interaction. 38, 45, 64

IAT Intelligent Assistive Technology. 34, 37, 40, 42, 62, 63

IoT Internet of Things. 11, 17, 47, 50, 51

PbD Privacy by Design. vii, ix, 23, 52, 53, 57–60, 63, 75, 79

PEB privacy enhancing behavior. 39, 44

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

PIA privacy impact assessment. 52, 59, 93

RIA robot impact assessment. 59

SAR Socially Assistive Robot. 9, 10

SIA surveillance impact assessment. 59

SSL Secure Sockets Layer. 59

UDHR Universal Declaration of Human Rights. 12, 13, 32

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Bibliography

Aghajan, Hamid, Juan Carlos Augusto, Chen Wu, Paul McCullagh, and Julie-Ann Walkden (2007). „Distributed vision-based accident management for assisted living“. In: ZSCC: 0000090. Springer, pp. 196–205.

Alaiad, Ahmad and Lina Zhou (2014). „The Determinants of Home Healthcare Robots Adoption: An Empirical Investigation“. In: *International journal of medical informatics* 83.11, pp. 825–840. ISSN: 1386-5056.

Allouch, Somaya Ben and Lex van Velsen (2020). „Social Robots for Elderly Care: An Inventory of Promising Use Cases and Business Models.“ In: *Studies in health technology and informatics* 270, pp. 1046–1050. ISSN: 0926-9630.

Armbrust, Christopher, Syed Atif Mehdi, Max Reichardt, Jan Koch, and Karsten Berns (2011). „Using an Autonomous Robot to Maintain Privacy in Assistive Environments“. In: *Security and Communication Networks* 4.11, pp. 1275–1293. ISSN: 1939-0114.

Bartoletti, Ivana (2019). „AI in Healthcare: Ethical and Privacy Challenges“. In: *Conference on Artificial Intelligence in Medicine in Europe*. Springer, pp. 7–10.

Blake, Valarie K. (2019). „Regulating Care Robots“. In: *Temp. L. Rev.* 92, p. 551.

Brandeis, Louis and Samuel Warren (1890). „The Right to Privacy“. In: *Harvard law review* 4.5, pp. 193–220.

Broadbent, Elizabeth, Jeff Garrett, Nicola Jepsen, Vickie Li Ogilvie, Ho Seok Ahn, Hayley Robinson, Kathryn Peri, Ngaire Kerse, Paul Rouse, and Avinesh Pillai (2018). „Using Robots at Home to Support Patients with Chronic Obstructive Pulmonary Disease: Pilot Randomized Controlled Trial“. In: *Journal of medical Internet research* 20.2, e8640.

Burgoon, Judee K (1982). „Privacy and Communication“. In: *Annals of the International Communication Association* 6.1, pp. 206–249. ISSN: 2380-8985.

Caine, Kelly, Selma Šabanovic, and Mary Carter (2012). „The Effect of Monitoring by Cameras and Robots on the Privacy Enhancing Behaviors of Older Adults“. In: *Proceedings of the Seventh Annual ACM/IEEE International Conference on Human-Robot Interaction*, pp. 343–350.

Calo, M. Ryan (2011). „Peeping Hals“. In: *Artificial Intelligence* 175.5-6, pp. 940–941. ISSN: 0004-3702.

— (2020). „12 Robots and Privacy“. In: *Machine Ethics and Robot Ethics*. Routledge, pp. 491–505. ISBN: 1-00-307499-5.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Carnevale, Antonio (2016). „Will Robots Know Us Better than We Know Ourselves?“ In: *Robotics and Autonomous Systems* 86, pp. 144–151. ISSN: 0921-8890.

Casey, Dympna, Heike Felzmann, Geoff Pegman, Christos Kouroupetroglou, Kathy Murphy, Adamantios Koumpis, and Sally Whelan (2016). „What People with Dementia Want: Designing MARIO an Acceptable Robot Companion“. In: *International Conference on Computers Helping People with Special Needs*. Springer, pp. 318–325.

Cavoukian, Ann (2010). „Privacy by Design: The Definitive Workshop. A Foreword by Ann Cavoukian, Ph. D“. In: *Identity in the Information Society* 3.2, pp. 247–251. ISSN: 1876-0678.

Coeckelbergh, Mark (2016). „Care Robots and the Future of ICT-Mediated Elderly Care: A Response to Doom Scenarios“. In: *AI & society* 31.4, pp. 455–462. ISSN: 1435-5655.

De Mauro, Andrea, Marco Greco, and Michele Grimaldi (2016). „A Formal Definition of Big Data Based on Its Essential Features“. In: *Library Review*. ISSN: 0024-2535.

van de Ven, Antoine AJ, Anne-mie AG Sponselee, and Ben AM Schouten (2010). „Robo MD: a home care robot for monitoring and detection of critical situations“. In: pp. 375–376.

Decker, Michael (2012). „Service Robots in the Mirror of Reflective Research“. In: *Poiesis & Praxis* 9.3, pp. 181–200. ISSN: 1615-6617.

Demiris, George, Debra Parker Oliver, Jarod Giger, Marjorie Skubic, and Marilyn Rantz (2009). „Older Adults' Privacy Considerations for Vision Based Recognition Methods of Eldercare Applications“. In: *Technology and Health Care* 17.1, pp. 41–48. ISSN: 0928-7329.

Denning, Tamara, Cynthia Matuszek, Karl Koscher, Joshua R Smith, and Tadayoshi Kohno (2009). „A Spotlight on Security and Privacy Risks with Future Household Robots: Attacks and Lessons“. In: *Proceedings of the 11th International Conference on Ubiquitous Computing*, pp. 105–114.

Dinh-Le, Catherine, Rachel Chuang, Sara Chokshi, and Devin Mann (2019). „Wearable Health Technology and Electronic Health Record Integration: Scoping Review and Future Directions“. In: *JMIR mHealth and uHealth* 7.9, e12861.

Draper, Heather and Tom Sorell (2017). „Ethical Values and Social Care Robots for Older People: An International Qualitative Study“. In: *Ethics and Information Technology* 19.1, p. 49. ISSN: 1388-1957.

Dubowsky, Steven, Frank Genot, Sara Godding, Hisamitsu Kozono, Adam Skwersky, Haoyong Yu, and Long Shen Yu (2000). „PAMM-A robotic aid to the elderly for mobility assistance and monitoring: a" helping-hand" for the elderly“. In: vol. 1. ZSCC: 0000353. IEEE, pp. 570–576. ISBN: 0-7803-5886-4.

van Dyck, Laura I, Kirsten M Wilkins, Jennifer Ouellet, Gregory M Ouellet, and Michelle L Conroy (2020). „Combating Heightened Social Isolation of Nursing Home Elders: The Telephone Outreach in the COVID-19 Outbreak Program“. In: *The American journal of geriatric psychiatry* 28.9, pp. 989–992. ISSN: 1064-7481.

Eklund, J Mikael, Jonathan Sprinkle, Shankar Sastry, and T Riisgaard Hansen (2006). „Information Technology for Assisted Living at Home: building a wireless infrastructure for assisted living“. In: ZSCC: 0000107. IEEE, pp. 3931–3934. ISBN: 0-7803-8741-4.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Fasola, Juan and Maja J Matarić (2010). „Robot Exercise Instructor: A Socially Assistive Robot System to Monitor and Encourage Physical Exercise for the Elderly“. In: *19th International Symposium in Robot and Human Interactive Communication*. IEEE, pp. 416–421. ISBN: 1-4244-7990-8.

— (2013). „A Socially Assistive Robot Exercise Coach for the Elderly“. In: *Journal of Human-Robot Interaction* 2.2, pp. 3–32. ISSN: 2163-0364.

Feil-Seifer, David and Maja J Matarić (2011). „Socially Assistive Robotics“. In: *IEEE Robotics & Automation Magazine* 18.1, pp. 24–31. ISSN: 1070-9932.

Felzmann, Heike, Timur Beyan, Mark Ryan, and Oya Beyan (2016). „Implementing an Ethical Approach to Big Data Analytics in Assistive Robotics for Elderly with Dementia“. In: *Acm Sigcas Computers and Society* 45.3, pp. 280–286. ISSN: 0095-2737.

Fernandes, Francisco Erivaldo, Guanci Yang, Ha Manh Do, and Weihua Sheng (2016). „Detection of Privacy-Sensitive Situations for Social Robots in Smart Homes“. In: *2016 IEEE International Conference on Automation Science and Engineering (CASE)*. IEEE, pp. 727–732. ISBN: 1-5090-2409-3.

Figueredo, MVM and JS Dias (2004). „Mobile telemedicine system for home care and patient monitoring“. In: vol. 2. ZSCC: 0000167. IEEE, pp. 3387–3390. ISBN: 0-7803-8439-3.

Fiske, Amelia, Peter Henningsen, and Alena Buyx (2019). „Your Robot Therapist Will See You Now: Ethical Implications of Embodied Artificial Intelligence in Psychiatry, Psychology, and Psychotherapy“. In: *Journal of medical Internet research* 21.5, e13216.

Fosch-Villaronga, E. (2015). „Creation of a Care Robot Impact Assessment“. In: *Int J Soc Behav Edu Econ Bus Ind Eng* 9, pp. 1913–1917.

Fosch-Villaronga, Eduard (2019). „Robots, Standards and the Law: Rivalries between Private Standards and Public Policymaking for Robot Governance“. In: *Computer Law & Security Review* 35.2, pp. 129–144. ISSN: 0267-3649.

Fosch-Villaronga, Eduard and Jordi Albo-Canals (2019). „“I'll Take Care of You,” Said the Robot“. In: *Paladyn, Journal of Behavioral Robotics* 10.1, pp. 77–93. ISSN: 2081-4836.

Fosch-Villaronga, Eduard and Adam Poulsen (2021). „Sex Robots in Care: Setting the Stage for a Discussion on the Potential Use of Sexual Robot Technologies for Persons with Disabilities“. In: *Companion of the 2021 ACM/IEEE International Conference on Human-Robot Interaction*, pp. 1–9.

Fosch-Villaronga, Eduard and Antoni Roig (2017). „European Regulatory Framework for Person Carrier Robots“. In: *Computer Law & Security Review* 33.4, pp. 502–520. ISSN: 0267-3649.

Fosch-Villaronga, Eduard, Aurelia Tamò-Larrieux, and Christoph Lutz (2018). „Did I Tell You My New Therapist Is a Robot? Ethical, Legal, and Societal Issues of Healthcare and Therapeutic Robots“. In: *Ethical, Legal, and Societal Issues of Healthcare and Therapeutic Robots (October 17, 2018)*.

Frik, Alisa, Leysan Nurgalieva, Julia Bernd, Joyce Lee, Florian Schaub, and Serge Egelman (2019). „Privacy and Security Threat Models and Mitigation Strategies of Older Adults“. In: *Fifteenth Symposium on Usable Privacy and Security ({SOUPS 2019)*, pp. 21–40. ISBN: 1-939133-05-X.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Furuta, Yoshitaka, Masayoshi Kanoh, Taro Shimizu, Masaru Shimizu, and Tsuyoshi Nakamura (2012). „Subjective Evaluation of Use of Babyloid for Doll Therapy“. In: *2012 IEEE International Conference on Fuzzy Systems*. IEEE, pp. 1–4. ISBN: 1-4673-1506-0.

García-Soler, Álvaro, David Facal, Unai Díaz-Orueta, Lucia Pigini, Lorenzo Blasi, and Renxi Qiu (2018). „Inclusion of Service Robots in the Daily Lives of Frail Older Users: A Step-by-Step Definition Procedure on Users' Requirements“. In: *Archives of gerontology and geriatrics* 74, pp. 191–196. ISSN: 0167-4943.

Gellman, Robert (2019). „Fair Information Practices: A Basic History-Version 2.19“. In: *Available at SSRN 2415020*. ZSCC: 0000010.

Gonzalez-Jimenez, Javier, Cipriano Galindo, and Carlos Gutierrez-Castaneda (2013). „Evaluation of a Telepresence Robot for the Elderly: A Spanish Experience“. In: *International Work-Conference on the Interplay Between Natural and Artificial Computation*. Springer, pp. 141–150.

Graf, Birgit, Matthias Hans, and Rolf D Schraft (2004). „Care-O-Bot II—Development of a next Generation Robotic Home Assistant“. In: *Autonomous robots* 16.2, pp. 193–205. ISSN: 1573-7527.

Graf, Birgit, Ulrich Reiser, Martin Hägele, Kathrin Mauz, and Peter Klein (2009). „Robotic Home Assistant Care-O-Bot® 3-Product Vision and Innovation Platform“. In: *2009 IEEE Workshop on Advanced Robotics and Its Social Impacts*. IEEE, pp. 139–144. ISBN: 1-4244-4393-8.

Gross, Horst-Michael, Steffen Mueller, Christof Schroeter, Michael Volkhardt, Andrea Scheidig, Klaus Debes, Katja Richter, and Nicola Doering (2015). „Robot Companion for Domestic Health Assistance: Implementation, Test and Case Study under Everyday Conditions in Private Apartments“. In: *2015 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*. IEEE, pp. 5992–5999. ISBN: 1-4799-9994-6.

van Heek, Julia, Simon Himmel, and Martina Ziefle (2017). „Privacy, Data Security, and the Acceptance of AAL-Systems–a User-Specific Perspective“. In: *International Conference on Human Aspects of IT for the Aged Population*. Springer, pp. 38–56.

Heuer, Tanja, Ina Schiering, and Reinhard Gerndt (2017). „Privacy and Socially Assistive Robots-a Meta Study“. In: *IFIP International Summer School on Privacy and Identity Management*. Springer, pp. 265–281.

Heuer, Tanja, Ina Schiering, and Reinhardt Gerndt (2018). „Transparency for Social Robots“. In:

Hoorn, Johan F, Elly A Konijn, Desmond M Germans, Sander Burger, and Annemiek Munneke (2015). „The In-between Machine“. In: *Proceedings of the International Conference on Agents and Artificial Intelligence-Volume 2*, pp. 464–469.

Huber, Lesa and L Jean Camp (2017). „User-Driven Design in Smart Homes: Ethical Aspects“. In: *Handbook of Smart Homes, Health Care and Well-Being*, pp. 93–103.

Ienca, Marcello and Eduard Fosch-Villaronga (2019). „Privacy and Security Issues in Assistive Technologies for Dementia“. In: *Intelligent Assistive Technologies for Dementia: Clinical, Ethical, Social, and Regulatory Implications*, p. 221. ISSN: 0190459816.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Ienca, Marcello, Tenzin Wangmo, Fabrice Jotterand, Reto W Kressig, and Bernice Elger (2018). „Ethical design of intelligent assistive technologies for dementia: a descriptive review“. In: *Science and engineering ethics* 24.4. ZSCC: 0000086 Publisher: Springer, pp. 1035–1055. ISSN: 1471-5546.

Isabet, Baptiste, Maribel Pino, Manon Lewis, Samuel Benveniste, and Anne-Sophie Rigaud (2021). „Social Telepresence Robots: A Narrative Review of Experiments Involving Older Adults before and during the COVID-19 Pandemic“. In: *International Journal of Environmental Research and Public Health* 18.7, p. 3597.

Ishii, Kaori (2019). „Comparative Legal Study on Privacy and Personal Data Protection for Robots Equipped with Artificial Intelligence: Looking at Functional and Technological Aspects“. In: *AI & SOCIETY* 34.3, pp. 509–533. ISSN: 1435-5655.

Jacobs, Theo and Gurvinder Singh Virk (2014). „ISO 13482-The New Safety Standard for Personal Care Robots“. In: *ISR/Robotik 2014; 41st International Symposium on Robotics*. VDE, pp. 1–6. ISBN: 3-8007-3601-2.

Jecker, Nancy S (2020). „You've Got a Friend in Me: Sociable Robots for Older Adults in an Age of Global Pandemics“. In: *Ethics and Information Technology*, pp. 1–9. ISSN: 1572-8439.

— (2021). „Nothing to Be Ashamed of: Sex Robots for Older Adults with Disabilities“. In: *Journal of Medical Ethics* 47.1, pp. 26–32. ISSN: 0306-6800.

Kaminski, Margot E. (2014). „Robots in the Home: What Will We Have Agreed To“. In: *Idaho L. Rev.* 51, p. 661.

Kok, Joost N, Egbert J Boers, Walter A Kosters, Peter Van der Putten, and Mannes Poel (2009). „Artificial Intelligence: Definition, Trends, Techniques, and Cases“. In: *Artificial intelligence* 1, pp. 270–299.

Koops, Bert-Jaap and Ronald Leenes (2005). „Code and the Slow Erosion of Privacy“. In: *Mich. Telecomm. & Tech. L. Rev.* 12, p. 115.

Kumar, Santosh, Wendy J Nilsen, Amy Abernethy, Audie Atienza, Kevin Patrick, Misha Pavel, William T Riley, Albert Shar, Bonnie Spring, and Donna Spruijt-Metz (2013). „Mobile Health Technology Evaluation: The mHealth Evidence Workshop“. In: *American journal of preventive medicine* 45.2, pp. 228–236. ISSN: 0749-3797.

Lammer, Lara, Andreas Huber, Astrid Weiss, and Markus Vincze (2014). „Mutual Care: How Older Adults React When They Should Help Their Care Robot“. In: *AISB2014: Proceedings of the 3rd International Symposium on New Frontiers in Human–Robot Interaction*. Routledge London, UK, pp. 1–4.

Lee, Min Kyung, Karen P Tang, Jodi Forlizzi, and Sara Kiesler (2011). „Understanding Users' Perception of Privacy in Human-Robot Interaction“. In: *2011 6th ACM/IEEE International Conference on Human-Robot Interaction (HRI)*. IEEE, pp. 181–182. ISBN: 1-4673-4395-1.

Li, Xiuquan and Tao Zhang (2017). „An Exploration on Artificial Intelligence Application: From Security, Privacy and Ethic Perspective“. In: *2017 IEEE 2nd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA)*. IEEE, pp. 416–420. ISBN: 1-5090-4499-X.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Lutz, Christoph, Maren Schöttler, and Christian Pieter Hoffmann (2019). „The privacy implications of social robots: Scoping review and expert interviews“. In: *Mobile Media & Communication* 7.3. ZSCC: 0000023, pp. 412–434. URL: https://journals.sagepub.com/doi/abs/10.1177/2050157919843961 (visited on 02/04/2021).

Lutz, Christoph and Aurelia Tamò (2015). „RoboCode-Ethicists: Privacy-friendly robots, an ethical responsibility of engineers?“ In: *Proceedings of the ACM Web Science Conference*. ZSCC: 0000024, pp. 1–12.

— (2016). „Privacy and healthcare robots–an ant analysis“. In: *We Robot*. ZSCC: 0000012.

Lutz, Christoph and Aurelia Tamó-Larrieux (2020). „The robot privacy paradox: Understanding how privacy concerns shape intentions to use social robots“. In: ZSCC: 0000012. ISSN: 2638-602X.

Marczak, Bill, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert (2018). *HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*. Tech. rep.

Martinez-Martin, Ester and Angel P del Pobil (2018). „Personal Robot Assistants for Elderly Care: An Overview“. In: *Personal assistants: Emerging computational technologies*, pp. 77–91.

Mell, Peter and Tim Grance (2011). „The NIST Definition of Cloud Computing“. In:

Mihas, Paul and Odum Institute (2019). *Learn to Build a Codebook for a Generic Qualitative Study*. SAGE Publications, Limited. ISBN: 1-5264-9605-4.

Mitzner, Tracy L, Julie B Boron, Cara Bailey Fausset, Anne E Adams, Neil Charness, Sara J Czaja, Katinka Dijkstra, Arthur D Fisk, Wendy A Rogers, and Joseph Sharit (2010). „Older Adults Talk Technology: Technology Usage and Attitudes“. In: *Computers in human behavior* 26.6, pp. 1710–1721. ISSN: 0747-5632.

Mukai, Toshiharu, Shinya Hirano, Hiromichi Nakashima, Yo Kato, Yuki Sakaida, Shijie Guo, and Shigeyuki Hosoe (2010). „Development of a Nursing-Care Assistant Robot RIBA That Can Lift a Human in Its Arms“. In: *2010 IEEE/RSJ International Conference on Intelligent Robots and Systems*. IEEE, pp. 5996–6001. ISBN: 1-4244-6676-8.

Muñoz, Andrés, Juan Carlos Augusto, Ana Villa, and Juan Antonio Botía (2011). „Design and evaluation of an ambient assisted living system based on an argumentative multi-agent system“. In: *Personal and Ubiquitous Computing* 15.4. ZSCC: 0000052 Publisher: Springer, pp. 377–387. ISSN: 1617-4909.

Nakashima, Toyoshiro, Goro Fukutome, and Naohiro Ishii (2010). „Healing Effects of Pet Robots at an Elderly-Care Facility“. In: *2010 IEEE/ACIS 9th International Conference on Computer and Information Science*. IEEE, pp. 407–412. ISBN: 1-4244-8198-8.

National Academies of Sciences, Engineering, and Medicine (2020). *Social Isolation and Loneliness in Older Adults: Opportunities for the Health Care System*. National Academies Press. ISBN: 0-309-67100-0.

Niemelä, Marketta, Lina Van Aerschot, Antti Tammela, and Iina Aaltonen (2017). „A Telepresence Robot in Residential Care: Family Increasingly Present, Personnel

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Worried about Privacy“. In: *International Conference on Social Robotics*. Springer, pp. 85–94.

Nissenbaum, Helen (2004). „Privacy as contextual integrity“. In: *Wash. L. Rev.* 79. ZSCC: 0002284 Publisher: HeinOnline, p. 119.

Novitzky, Peter, Alan F Smeaton, Cynthia Chen, Kate Irving, Tim Jacquemard, Fiachra O'Brolcháin, Dónal O'Mathúna, and Bert Gordijn (2015). „A Review of Contemporary Work on the Ethics of Ambient Assisted Living Technologies for People with Dementia“. In: *Science and engineering ethics* 21.3, pp. 707–765. ISSN: 1471-5546.

Pagallo, Ugo (2013). „Robots in the Cloud with Privacy: A New Threat to Data Protection?“ In: *Computer Law & Security Review* 29.5, pp. 501–508. ISSN: 0267-3649.

Palen, Leysia and Paul Dourish (2003). „Unpacking" privacy" for a networked world“. In: ZSCC: 0001299, pp. 129–136.

Pensas, Harri, Antti-Matti Vainio, Markus Garschall, Tero Kivimäki, Stratis Konakas, Socrates Costicoglou, and Jukka Vanhala (2014). „Using ambient communication and social networking technologies to reduce loneliness of elders“. In: ZSCC: 0000004. Springer, pp. 91–102.

Pollack, Martha E, Laura Brown, Dirk Colbry, Colleen E McCarthy, Cheryl Orosz, Bart Peintner, Sailesh Ramakrishnan, and Ioannis Tsamardinos (2003). „Autominder: An intelligent cognitive orthotic system for people with memory impairment“. In: *Robotics and autonomous systems* 44.3-4. ZSCC: 0000461 Publisher: Elsevier, pp. 273–282. ISSN: 0921-8890.

Pollack, Martha E, Laura Brown, Dirk Colbry, Cheryl Orosz, Bart Peintner, Sailesh Ramakrishnan, Sandra Engberg, Judith T Matthews, Jacqueline Dunbar-Jacob, and Colleen E McCarthy (2002). „Pearl: A Mobile Robotic Assistant for the Elderly“. In: *AAAI Workshop on Automation as Eldercare*. Vol. 2002, pp. 85–91.

Poulsen, Adam and Oliver K. Burmeister (2019). „Overcoming carer shortages with care robots: Dynamic value trade-offs in run-time“. In: *Australasian Journal of Information Systems* 23. ZSCC: 0000031 ISBN: 1449-8618 Publisher: Australian Computer Society.

Redfoot, Donald, Lynn Feinberg, and Ari N Houser (2013). *The Aging of the Baby Boom and the Growing Care Gap: A Look at Future Declines in the Availability of Family Caregivers*. AARP Public Policy Institute Washington, DC.

Reinhardt, Delphine, Monisha Khurana, and Luca Hernández Acosta (2021). „“I Still Need My Privacy”: Exploring the Level of Comfort and Privacy Preferences of German-Speaking Older Adults in the Case of Mobile Assistant Robots“. In: *Pervasive and Mobile Computing* 74, p. 101397. ISSN: 1574-1192.

Rincon, JA, Javier Palanca, V Botti, A Costa, Paulo Novais, Vicente Julian, and Carlos Carrascosa (2019). „EMiR 2.0: A Cognitive Assistant Robot for Elderly“. In: *International Conference on Practical Applications of Agents and Multi-Agent Systems*. Springer, pp. 273–276.

Rueben, Matthew, Alexander Mois Aroyo, Christoph Lutz, Johannes Schmölz, Pieter Van Cleynenbreugel, Andrea Corti, Siddharth Agrawal, and William D Smart (2018). „Themes and Research Directions in Privacy-Sensitive Robotics“. In: *2018 IEEE*

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Workshop on Advanced Robotics and Its Social Impacts (ARSO). IEEE, pp. 77–84. ISBN: 1-5386-8037-8.

Ryan, Lindsay H, Jacqui Smith, Toni C Antonucci, and James S Jackson (2012). „Cohort Differences in the Availability of Informal Caregivers: Are the Boomers at Risk?“ In: *The Gerontologist* 52.2, pp. 177–188. ISSN: 1758-5341.

Saldaña, Johnny (2013). *The Coding Manual for Qualitative Researchers*. Second. sage. ISBN: 978-1-4462-4736-5.

Schafer, Burkhard and Lilian Edwards (2017). „“I spy, with my little sensor”: fair data handling practices for robots between privacy, copyright and security“. In: *Connection Science* 29.3. ZSCC: 0000016 Publisher: Taylor & Francis, pp. 200–209. ISSN: 0954-0091.

Schoeman, Ferdinand (1984). „Privacy: Philosophical Dimensions“. In: *American Philosophical Quarterly* 21.3, pp. 199–213. ISSN: 0003-0481.

Schomakers, Eva-Maria and Martina Ziefle (2019). „Privacy Perceptions in Ambient Assisted Living.“ In: ZSCC: 0000009, pp. 205–212.

Schulz, Trenton, Jo Herstad, and Harald Holone (2018). „Privacy at home: an inquiry into sensors and robots for the stay at home elderly“. In: ZSCC: 0000008. Springer, pp. 377–394.

Sedenberg, Elaine, John Chuang, and Deirdre Mulligan (2016). „Designing Commercial Therapeutic Robots for Privacy Preserving Systems and Ethical Research Practices within the Home“. In: *International Journal of Social Robotics* 8.4, pp. 575–587. ISSN: 1875-4805.

Sharkey, Amanda and Noel Sharkey (2012). „Granny and the robots: ethical issues in robot care for the elderly“. In: *Ethics and information technology* 14.1. ZSCC: 0000719 Publisher: Springer, pp. 27–40. ISSN: 1572-8439.

Sharkey, Noel and Amanda Sharkey (2011). „17 the rights and wrongs of robot care“. In: *Robot ethics: The ethical and social implications of robotics*. ZSCC: 0000063, p. 267.

Simard, Joyce and Ladislav Volicer (2020). „Loneliness and Isolation in Long-Term Care and the COVID-19 Pandemic“. In: *Journal of the American Medical Directors Association* 21.7, pp. 966–967. ISSN: 1525-8610.

Simshaw, Drew, Nicolas Terry, Kris Hauser, and ML Cummings (2015). „Regulating healthcare robots: Maximizing opportunities while minimizing risks“. In: *Rich. JL & Tech.* 22. ZSCC: 0000029 Publisher: HeinOnline, p. 1.

Theoharidou, M, N Tsalis, and D Gritzalis (2017). „Smart Home Solutions: Privacy Issues“. In: *Handbook of Smart Homes Health Care and Well-Being*. ZSCC: 0000002 Publisher: Springer New York, NY, pp. 67–81.

Thorstensen, Erik (2018). „Privacy and future consent in smart homes as assisted living technologies“. In: ZSCC: 0000005. Springer, pp. 415–433.

Townsend, Daphne, Frank Knoefel, and Rafik Goubran (2011). „Privacy versus Autonomy: A Tradeoff Model for Smart Home Monitoring Technologies“. In: *2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*. IEEE, pp. 4749–4752. ISBN: 1-4577-1589-9.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Tzafestas, Spyros G (2018). „Roboethics: Fundamental Concepts and Future Prospects“. In: *Information* 9.6, p. 148.

Umetani, Tomohiro, Satoshi Aoki, Kazuhiro Akiyama, Ryo Mashimo, Tatsuya Kitamura, and Akiyo Nadamoto (2016). „Scalable Component-Based Manzai Robots as Automated Funny Content Generators“. In: *Journal of Robotics and Mechatronics* 28.6, pp. 862–869. ISSN: 0915-3942.

Umetani, Tomohiro, Ryo Mashimo, Akiyo Nadamoto, Tatsuya Kitamura, and Hirotaka Nakayama (2014). „Manzai Robots: Entertainment Robots Based on Auto-Created Manzai Scripts from Web News Articles“. In: *Journal of Robotics and Mechatronics* 26.5, pp. 662–664. ISSN: 0915-3942.

United Nations, Department of Economic and Social Affairs, Population Division (2019a). *World Population Ageing 2019: Highlights*. ST/ESA/SER.A/430. ISBN: 978-92-1-148325-3.

— (2019b). *World Population Prospects 2019: Volume I: Comprehensive Tables*. ST/ESA/SER.A/430. ISBN: 978-92-1-148327-7.

Vallverdú, Jordi and David Casacuberta (2015). „Ethical and Technical Aspects of Emotions to Create Empathy in Medical Machines“. In: *Machine Medical Ethics*. Springer, pp. 341–362.

Vandemeulebroucke, Tijs, Bernadette Dierckx de Casterlé, and Chris Gastmans (2018). „The Use of Care Robots in Aged Care: A Systematic Review of Argument-Based Ethics Literature“. In: *Archives of gerontology and geriatrics* 74, pp. 15–25. ISSN: 0167-4943.

Vandemeulebroucke, Tijs, Kevin Dzi, and Chris Gastmans (2021). „Older Adults' Experiences with and Perceptions of the Use of Socially Assistive Robots in Aged Care: A Systematic Review of Quantitative Evidence“. In: *Archives of Gerontology and Geriatrics*, p. 104399. ISSN: 0167-4943.

Wada, Kazuyoshi, Takanori Shibata, Tomoko Saito, and Kazuo Tanie (2003). „Effects of Robot Assisted Activity to Elderly People Who Stay at a Health Service Facility for the Aged“. In: *Proceedings 2003 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS 2003)(Cat. No. 03CH37453)*. Vol. 3. IEEE, pp. 2847–2852. ISBN: 0-7803-7860-1.

Wang, Hua, Cuiqin Ma, and Lijuan Zhou (2009). „A Brief Review of Machine Learning and Its Application“. In: *2009 International Conference on Information Engineering and Computer Science*. IEEE, pp. 1–4. ISBN: 1-4244-4994-4.

Westin, Alan F (1968). „Privacy and Freedom“. In: *Washington and Lee Law Review* 25.1, p. 166. ISSN: 0043-0463.

Wortmann, Felix and Kristina Flüchter (2015). „Internet of Things“. In: *Business & Information Systems Engineering* 57.3, pp. 221–224. ISSN: 2363-7005.

Wu, Xian, Lauren C Nix, Amanda M Brummett, Cynthia Aguillon, Danielle J Oltman, and Jenay M Beer (2021). „The Design, Development, and Evaluation of Telepresence Interfaces for Aging Adults: Investigating User Perceptions of Privacy and Usability“. In: *International Journal of Human-Computer Studies*, p. 102695. ISSN: 1071-5819.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN

Xiao, Yu and Maria Watson (Mar. 2019). „Guidance on Conducting a Systematic Literature Review“. In: *Journal of Planning Education and Research* 39.1, pp. 93–112. ISSN: 0739-456X. DOI: 10.1177/0739456X17723971.

Yamazaki, Kimitoshi, Ryohei Ueda, Shunichi Nozawa, Mitsuharu Kojima, Kei Okada, Kiyoshi Matsumoto, Masaru Ishikawa, Isao Shimoyama, and Masayuki Inaba (2012). „Home-Assistant Robot for an Aging Society“. In: *Proceedings of the IEEE* 100.8, pp. 2429–2441. ISSN: 0018-9219.

Yan, Hairong, Li Da Xu, Zhuming Bi, Zhibo Pang, Jie Zhang, and Yong Chen (2015). „An Emerging Technology–Wearable Wireless Sensor Networks with Applications in Human Health Condition Monitoring“. In: *Journal of Management Analytics* 2.2, pp. 121–137. ISSN: 2327-0012.

Yang, Daseul, Yu-Jung Chae, Doogon Kim, Yoonseob Lim, Dong Hwan Kim, ChangHwan Kim, Sung-Kee Park, and Changjoo Nam (2021). „Effects of Social Behaviors of Robots in Privacy-Sensitive Situations“. In: *International Journal of Social Robotics*, pp. 1–14. ISSN: 1875-4805.

Yang, Guanci, Jing Yang, Weihua Sheng, Francisco Erivaldo Fernandes Junior, and Shaobo Li (2018). „Convolutional Neural Network-Based Embarrassing Situation Detection under Camera for Social Robot in Smart Homes“. In: *Sensors* 18.5, p. 1530.

Yusif, Salifu, Jeffrey Soar, and Abdul Hafeez-Baig (2016). „Older People, Assistive Technologies, and the Barriers to Adoption: A Systematic Review“. In: *International journal of medical informatics* 94, pp. 112–116. ISSN: 1386-5056.

Zhang, WJ, Guosheng Yang, Yingzi Lin, Chunli Ji, and Madan M Gupta (2018). „On Definition of Deep Learning“. In: *2018 World Automation Congress (WAC)*. IEEE, pp. 1–5. ISBN: 1-5323-7791-6.

Die approbierte gedruckte Originalversion dieser Diplomarbeit ist an der TU Wien Bibliothek verfügbar
The approved original version of this thesis is available in print at TU Wien Bibliothek.
TU Bibliothek Your knowledge hub WIEN