Research Article

Tanja Heuer*, Ina Schiering, and Reinhard Gerndt

Privacy framework for context-aware robot development

https://doi.org/10.1515/pjbr-2021-0032
received March 31, 2021; accepted November 10, 2021

Abstract: Privacy is an essential topic in (social) robotics and becomes even more important when considering interactive and autonomous robots within the domestic environment. Robots will collect a lot of personal and sensitive information about the users and their environment. Thereby, privacy does consider the topic of (cyber-) security and the protection of information against misuse by involved service providers. So far, the main focus relies on theoretical concepts to propose privacy principles for robots. This article provides a privacy framework as a feasible approach to consider security and privacy issues as a basis. Thereby, the proposed privacy framework is put in the context of a user-centered design approach to highlight the correlation between the design process steps and the steps of the privacy framework. Furthermore, this article introduces feasible privacy methodologies for privacy-enhancing development to simplify the risk assessment and meet the privacy principles. Even though user participation plays an essential role in robot development, this is not the focus of this article. Even though user participation plays an essential role in robot development, this is not the focus of this article. The employed privacy methodologies are showcased in a use case of a robot as an interaction partner contrasting two different use case scenarios to encourage the importance of context awareness.

Keywords: privacy framework, DPIA, privacy by design, social robot, context awareness, trust, privacy-enhancement

*** Corresponding author: Tanja Heuer,** Department of Computer Science, Ostfalia University of Applied Sciences, Institute of Information Engineering, Wolfenbüttel, Germany, e-mail: ta.heuer@ostfalia.de
Ina Schiering: Department of Computer Science, Ostfalia University of Applied Sciences, Institute of Information Engineering, Wolfenbüttel, Germany, e-mail: i.schiering@ostfalia.de
Reinhard Gerndt: Department of Computer Science, Ostfalia University of Applied Sciences, Institute of Distributed Systems, Wolfenbüttel, Germany, e-mail: r.gerndt@ostfalia.de

1 Introduction

Social robots become increasingly present within the domestic environment, for service tasks as well as for educational and entertainment purposes [1]. Robots will be part of our daily lives soon, and their tasks will not only be related to household tasks such as vacuum cleaning or lawn mowing. Moreover, they will become an assistant in a variety of daily life situations. Several studies examined preferred features for a robot and identified tasks such as reminders, information provision, healthcare supervision, cooking assistance, cognitive and social support, conversational dialogues, music playing, smart home integration, entertainment, and much more [2–4]. Therefore, robots are commonly equipped with various sensors such as cameras or microphones and are connected to the Internet to access information. These sensors allow the robot to perceive its environment to move around and interact with the inhabitants to provide assistance [5]. The way of robot behavior within the home context raises new ethical challenges and risks that need to be addressed [6,7].

These concerns include, e.g., autonomy, responsibility, trust, loss of control, loss of privacy, loss of personal liberty, and ethical considerations towards the human–robot relationship [8–11]. Most of the mentioned ethical concerns are strongly related to privacy. The more tasks and features a robot provides, the more extensive and complex the amount of collected data becomes. A simple vacuum cleaning robot cleans the floor in a random way. In contrast, a smart vacuum cleaning robot with additional sensors for obstacle recognition and home mapping can gain data about the whole domestic environment. Being additionally able to start the robot via other smart home devices provides data about other devices within the network [12].

The robots can move around autonomously and record whenever and wherever they want. Thereby, the gathered and processed information might consists of sensitive data of users, not only about the users themselves but also about their environment [13]. The robot will know about habits,

preferences, hobbies, diseases, and personal facts about the user. Furthermore, the robot maps the home and controls smart home elements. The robot taking control over other systems leads to the discussion of safeguarding this sensitive information and calls for responsible privacy-protecting research.

Privacy does not only concern threats from outside, (cyber-)attacks, or hackers. In addition, risks imposed by robot manufacturers and service providers have to be considered, e.g., misuse or unauthorized selling of data [14]. Privacy and data protection are fundamental human rights established in the Charter of Fundamental Rights of the EU. Furthermore, the processing of personal data needs to be transparent for users, and processing needs to be lawful. The principles of purpose limitation and data minimization need to be followed ref. [15]. This limitation means that the companies providing the robot and its services cannot track everything they want, but a specific purpose is required. The general data protection regulation (GDPR) [16] enforces a mindful confrontation with privacy-respecting development to ensure the rights of users in the EU. Responsible research means that ethical principles, as well as privacy, need to be a central part of the development process besides safety and security [17]. The *"pervasiveness and intrusiveness of robots"* in the home environment require a conscious examination of critical situations to minimize potential risks [18].

In this article, a privacy framework is proposed in the context of a domestic robot. Privacy methodologies from general IT services are adapted to present a practice-oriented concept for the Privacy by Design (PbD) principles [19]. The privacy framework is related to a user-centered design concept to provide an overview of interrelated stages. Although the user plays an important role, user involvement will not be the focus of this article. However, the focus is solely on the methodologies that simplify a risk assessment according to privacy. The privacy framework aims at a risk assessment for social robots, besides safety and security issues. Thereby, methods are presented to meet the principles for privacy-respecting development.

Following, Section 2 gives an overview of existing privacy principles for service robots. The main concepts turned out to be theoretical approaches without specific instructions, whereas they equate privacy with security and only focus on threats from outside. Section 3 proposes the stages of the risk management cycle and introduces the important methodologies. The proposed process and the methods are then exemplary demonstrated on a use case. A robot capable of social interaction and cognitive support is taken as a use case scenario to emphasize the importance of data protection. The importance of privacy in the context of robots' sensors, integrated services for data processing, and user information derived in such a scenario is provided.

2 Privacy principles in the context of social robots

As privacy for social robots, especially for the home context, gains more and more interest, there are various ideas and first approaches to taking care of this topic. A first concept was provided by Denning et al. [20]. A list of questions shall identify specific privacy- and security-related aspects that need to be considered for design decisions. The questions concentrate on social, environmental, and technical factors such as intended functionalities, users and context, actuators and sensors, and the threatening of privacy, physical integrity, physical safety, or psychological vulnerabilities.

Other concepts focus on risks that various sensors imply [21–24]. Lera et al. classify sensors according to the level of *"privacy leakage"* ranging from 1 to 5 (very low to very high) with the focus on disclosure of personal and environmental information [21]. A camera is classified as level 4 as it can disclose private images of the person and the environment. It is pointed out that a fusion of several sensors is considered the most dangerous. In addition, it is important to consider where data processing is conducted, as recorded raw images need to be analyzed. Eick and Anton do not only point out potential risks but also highlight the importance of sensor selection [24]. Researchers and developers must select the required sensors carefully depending on the identified requirements and the specified context. The aim is only to select the sensors that are needed. A careful sensor selection was already emphasized in the context of integration of a privacy-relevant model for robotic development [23]. Cerrudo and Apa gave additional examples of potential risks in private homes of certain sensors such as espionage or smart home manipulation [22].

Furthermore, within a workshop conducted by Rueben et al., the topic of privacy was categorized into seven relevant specified research fields [25]: *"data privacy; manipulation and deception; trust; blame and transparency; legal issues; domains with special privacy concerns; and privacy theory."* As the main focus for legal issues, they highlighted a so-called *"privacy education for users."* The importance of interdisciplinary collaboration is additionally emphasized.

An exchange across disciplines is beneficial, as shown with the PbD principle. The original PbD approach was developed by Cavoukian et al. [19]. The concept encompasses seven essential design principles for privacy. The seven principles are meant to establish basic rules for meaningful development. The PbD concept is discussed contrary as the complexity and variability of privacy issues are not discussed, and systematic methods are not appointed, which can be used to identify certain risks [26,27]. Nevertheless, this generalized and theoretical design concept was adapted in the context of robots for domestic use by the lawyer Pagallo called robot-cloud by design [28]:

(1) "We have to view data protection in proactive rather than reactive terms, making PbD preventive and not simply remedial.
(2) Personal data should be automatically protected in every robotic system as its default position.
(3) Data protection should consequently be embedded into the design of the application.
(4) The full functionality of the principle which follows from (2) and (3), allows a positive–sum or win–win game, making trade-offs unnecessary (e.g., privacy vs security).
(5) A cradle-to-grave, start-to-finish, or end-to-end life cycle protection ensures that privacy safeguards are at work even before a single bit of information has been collected by the machine.
(6) No matter the technology or business practices involved, the design project should make data protection mechanisms visible and transparent to both robotic users and providers.
(7) Finally, the principle "requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options" [19]. In other words, robot-cloud by design requires individual-focused respect for user privacy."

This overview shows that there are already existing theoretical concepts and approaches which outline the important issues for privacy-sensitive and privacy-respecting robotics. Nevertheless, there are no specified and formalized models and methodologies that put the theoretical approaches into practice in the context of social robots. The realizability and practical use of the proposed approaches are missing in the complex field of robotics. Furthermore, the theoretical approaches are insufficient regarding privacy as security issues foreground the concepts. Privacy is not only about risks from outside and being threatened by hackers or data theft. Moreover, it is about protecting sensitive information towards the robot manufacturer and accompanied service providers against, e.g., misuse [29]. Hence, this is an important research area in the context of social robotics. In the next section, further details are provided about PbD in general and methodologies as a basis for a quantified assessment.

3 Risk management cycle

As the PbD approach already proposes, the integration of privacy concepts is of fundamental importance. Methodologies from standard IT services are transferred to fit the needs for the development of social robots to propose a practice-based concept and ensure a privacy-sensitive and privacy-respecting development. The chosen methodologies for privacy enhancement are embedded into a risk management cycle consisting of the three steps: *risk identification*, *risk analysis*, and *risk mitigation*. This risk-based approach can also be applied in the context of a Data Protection Impact Assessment (DPIA) addressing the relevant steps and methods to be used for risk assessment [30,31]. Figure 1 shows the relevance of the risk management cycle in relation to the five steps of the design thinking process [32]. The design thinking process serves to clarify the correlation of process steps and the provided methodologies for privacy. Mainly, the design thinking process steps are similar to the development process steps of the ISO9241-210. It is mentioned that the user should play an essential decision-making role and is meant to participate during the entire cycle actively. Participation means that the user can express potential concerns and be made aware of other risks. But this is not the focus of this article, as it aims to propose the methodologies for risk

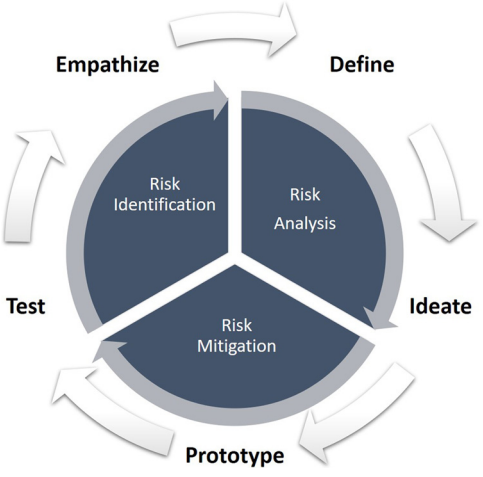

Figure 1: Privacy framework integrated into the design thinking process.

assessment in robotics. Thereby, the three steps of the privacy framework pursue the goals:

- Risk identification carves out potential privacy risks of defined functionalities based on necessary sensors and required information.
- Risk analysis as a second step deals with a reasonable measurement of benefits and risks and the analysis of privacy requirements for the chosen development concepts.
- Adequate measures for privacy protection meet the analyzed privacy requirements and need to be determined and implemented in the step of risk mitigation.

3.1 Risk identification – Seven types of privacy

The first step aims to identify privacy risks for the potential features of the social robot. In this case, it will be specified on the complex environment of the domestic home. To be able to identify all relevant privacy issues for the specific use case, the model *Seven types of privacy* by Finn et al. are used [33]. The model proposes a more complex approach than the two privacy distinctions of personal and environmental information made by Lera et al. [21]. This distinction gives the ability to foster the identification of specific risks more precisely. The types of privacy are defined in the following:

- **Privacy of the Person** covers the right of physical integrity, and this includes genetic and health data, medical conditions, and all data in terms of body functions of a person.
- **Privacy of Action and Behavior** is related to private information about daily habits, activities, preferences, and personal attitudes.
- **Privacy of Communication** affects the privacy of information through communication channels, including e-mails, calls, or messages.
- **Privacy of Data and Image** focus on the privacy of images and videos and that only the owners themselves can control the use.
- **Privacy of Thoughts and Feelings** means that information related to thoughts and feelings be kept private. It needs to be pointed out that thoughts and behavior do not always lead to the same outcomes.
- **Privacy of Location and Space** prohibits unauthorized tracking or monitoring of a person.
- **Privacy of the Association** takes care of connections and relations between individuals. Furthermore, this involves the content of personal conversations.

Transferred to the topic of robotics, the distinction of these types becomes even more important as social robots soon shall be seen and treated as friends. Robots as friends are only acceptable and ethically justifiable if the user can ensure that sensitive information is protected against threats and misuse. Even though the types are classified, often they cannot be wholly treated independently as, e.g., *privacy of data and image* can be connected to *privacy of location and space* as the environment is visible on the photos. As social robots will very likely act autonomously in the domestic environment, they will collect information at any time and any place.

3.2 Risk analysis – Privacy protection goals

In a second step, the privacy requirements for the selected use case need to be analyzed. In robotics so far, the security CIA model is used, which involves the need of *confidentiality, integrity, and availability*, and hence called the CIA model [34]. A common model in privacy engineering is the *privacy protection goals* [35]. The *privacy protection goals* extend the CIA model by the privacy goals *unlinkability/data minimization, transparency*, and *intervenability*. These protection goals are directly related to the GDPR. The six protection goals concentrate on the following:

- **Confidentiality** specifies that the data are treated discreetly and confidentially. Typical measures are, e.g., authentication and encryption.
- **Integrity** deals with the correctness of data and information. Correctness means that software, as well as hardware components, should be protected against unauthorized modifications.
- **Availability** addresses reasonable robustness and availability of the system. Availability involves the retrieval of information as well as the functionalities themselves.
- **Unlinkability** + **data minimization** describes the type of storage of collected data. Furthermore, the stored data should be reduced to the necessary minimum.
- **Transparency** implies the full transparency of functionality, using sensors and information, the process of data processing toward the user.
- **Intervenability** means that the user can decide whether sensors are allowed to record information and which features are turned on or off.

Even though all *protection goals* are important, it needs to be clarified that an implementation cannot fulfill

all six goals at the highest protection level at the same time. Therefore, requirements for an adequate level of privacy need to be carefully prioritized for every use case. Availability might conflict with confidentiality as availability measures might need to allow permanent access rights; what confidentiality measures try to prohibit or limit access rights. The same conflict occurs when intervenability and integrity or transparency and unlinkability are contrasted. Integrity tries to prohibit modifications – intervenability, on the other hand, focuses on user intervention. As a result, the user input must be verified according to correctness and permission, e.g., medication change as a case-sensitive example.

3.3 Risk mitigation

For the identified privacy risks and the defined privacy requirements, appropriate measures need to be figured out. Risk mitigation is a continuous process. The robot prototype with its features and capabilities needs to be tested and monitored regularly to prove sustainability or necessary adaptions and adjustments. Thereby, testing is not only about usability, operability, and usefulness. Moreover, it is about strategies that prevent the occurrence of the identified risks.

In robotics, Yong et al. proposed risk mitigation strategies, especially for wi-fi-enabled robot toys, e.g., parental control mechanisms, wireless connection, and camera protection strategies [36]. These strategies gave first hints of protection strategies. In contrast to the two previous steps, no specific model for mitigation exists so far to get an overall view for this process with all possible existing mitigation strategies as it consists of many different possible solutions.

Nevertheless, the standard data protection model does already provide a catalog of privacy measures that are divided into modules according to the risks (https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V2.0b.pdf). Overall, to find one or more suitable measures within the modules, they are split into the three categories: *data level, system level, and process level.*

4 Privacy framework

The use case of an interactive robot will be investigated as an example, and two use case scenarios are contrasted to highlight the importance of context awareness for privacy development. The robot can interact and talk with the user as a friend. It can recognize the user and customize its behavior and conversational content. Moreover, we can think of an advanced smart assistance device equipped with a camera (and can move autonomously). As this use case focuses on investigating privacy risks accompanied by the requirement of social and verbal interaction, the exploration of risks that correlate with autonomous movement will not be presented in detail in this article.

4.1 Risk identification

At the beginning of a development process, it is about the identification of needs and requirements. Thereby, the first step *empathize* of the design thinking process concentrates on the understanding of all constraints that are involved, such as target group, context, and resulting requirements. Risk identification determines potential risks for every identified need, connected to the *empathize* step.

Given the example of an interaction partner, which is a universal requirement, potential risks need to be figured out. As a specific interaction example, the features that have already been identified as needs are used [2–4,37]. These features require certain capabilities of the robot. The two main requirements that the interactive robot is meant to fulfill as a communicative interaction partner are **voice recording** and **informational processing and access** to be able to answer appropriately. An essential feature for an interaction partner is the ability to record and analyze voice. The most relevant sensor for this requirement is at least one microphone. Furthermore, user recognition shall be a fundamental part of the robot. This can be implemented in various ways, which are explained in the relevant subsection in more detail.

4.1.1 Voice recording

For voice and speech recognition, at least one microphone is required. The amount of sensors does not influence the potential risks. All recorded information should be classified as sensitive. Table 1 gives an overview of the potential risks. An installed microphone can imply privacy risks concerning the types *action and behavior, communication, thoughts and feelings, location, and space and association*. *Privacy of communication* is always affected as the robot is used as an interaction partner. The other privacy types can be affected depending on the content of the robot. The main issue is not the fact that the user is being

Table 1: Types of privacy risks in relation to sensors: (1) privacy of the person; (2) privacy of action and behavior; (3) privacy of communication; (4) privacy of data and image; (5) privacy of thoughts and feelings; (6) privacy of location and space; (7) privacy of association

Sensor	1	2	3	4	5	6	7
Microphone		X	X		X	X	X
Camera		X		X		X	X

recorded. It is about the type of information and its sensitivity that are recorded. Additional features that utilize sensitive information via speech-based commands induce further risks (Figure 2). A connected calendar to manage appointments provides information about *action and behavior* or *location and space*. The ability to make calls via this robot gives information about *associations*. Cooking aid provides information about possible intolerances. These risks do not imply that no feature should be realized. However, as any feature causes risks, protection has to be ensured.

4.1.2 User recognition

As mentioned earlier, there are different possibilities to realize user recognition. As a microphone is an essential sensor, this could be easily done by speech recognition [38]. A microphone is not sufficient in this context to pave the way for a context-sensitive robot. As an additional advantage, the robot should recognize a person, e.g., when entering a room, or the robot should be able to identify situations where it is advisable to offer support or call for help. These additional requirements ask for a camera. Section 3.2 defines the risks going along with an integrated camera. The features that enable the robot to react and behave situationally also entail privacy risks. *Privacy of data and image* is endangered, as well as *action and behavior*, *location and space*, and *associations*. Privacy of associations is at risk if, e.g., the robot recognizes persons like relatives or friends besides the users.

4.1.3 Informational process and access

The recorded information needs to be processed and analyzed to make the robot answer a question or fulfill a given task. Depending on the task, some features can be processed locally, such as reminders and timers – complex verbal interactions demand significantly more computational resources. They are typically provided externally for efficient processing. Besides identifying single words and sentences, additional information needs to be derived as the context of the sentence and possible background information, the pitch of the voice, and much more. Hence, as the number of features for which local processing power is sufficient is minimal, it is not discussed further. The analysis of the recorded voice data can lead to integrating additional providers, e.g., music streaming services, which also require privacy measures. Playing music would require a connection to streaming services, and weather and news reports need internet access to retrieve the up-to-date information. The discussion of a social robot with overall interaction capabilities implies gathering information about the users, habits, and life situations. On the basis of this pool of data, the robot can establish a meaningful conversation.

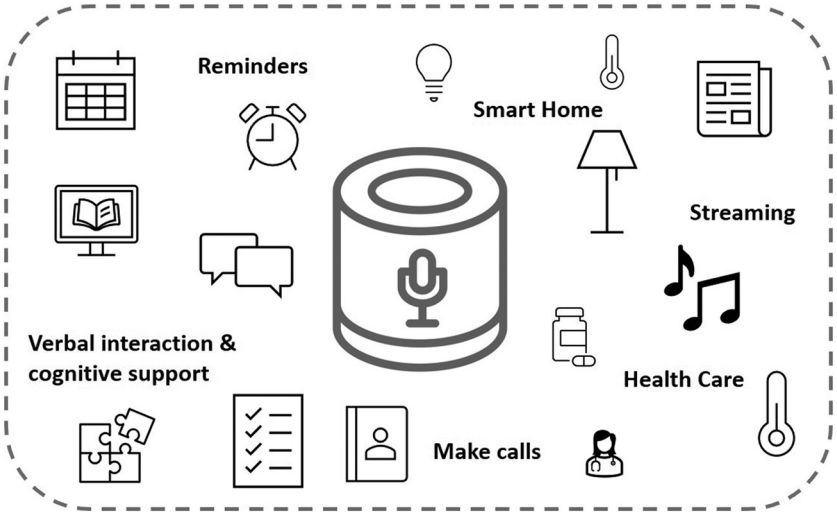

Figure 2: Robot companion that can be used for informational services and for social interaction.

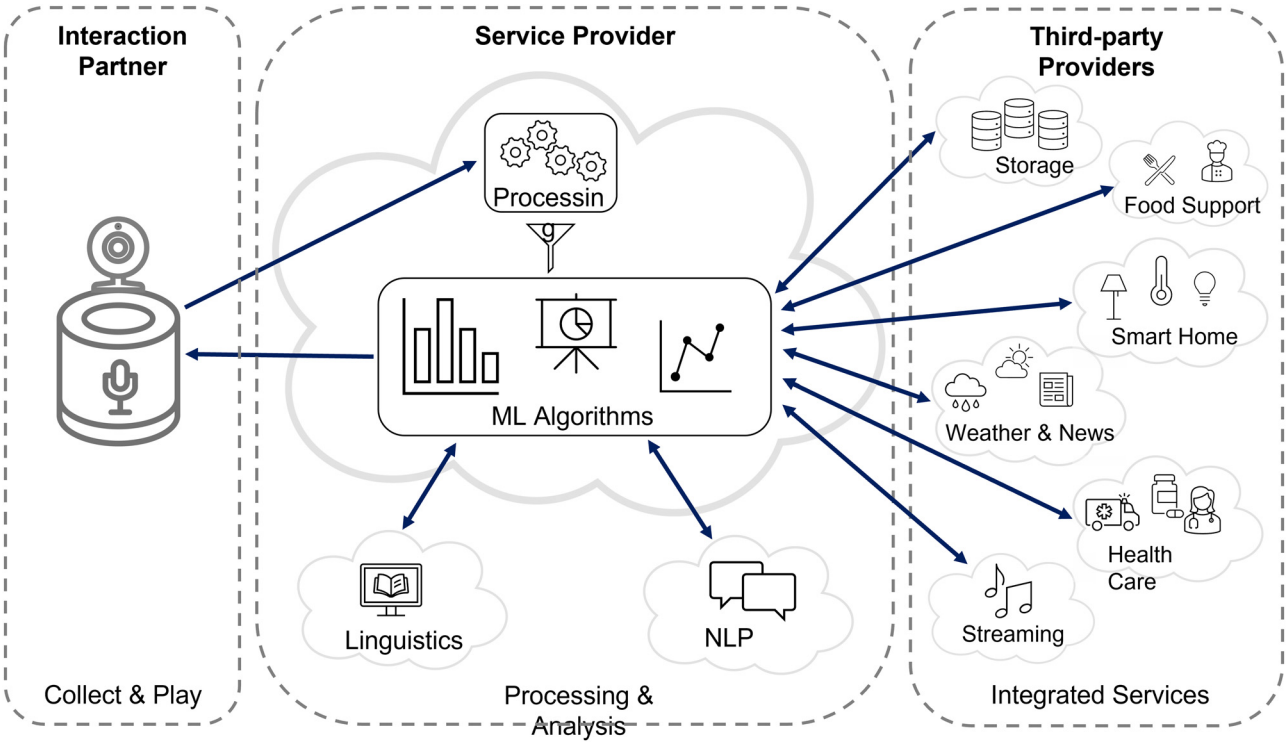

Figure 3: Interaction of service providers based on data processing and the flow of informations. ML, machine learning, NLP, natural language processing.

A simplified procedure for data processing, storage, and integrated services is presented in Figure 3. It gives an overview of potentially involved parties and providers of a robotic system and how they exchange information. The recorded raw data are sent to the cloud or another external server of one of the involved providers. The information is analyzed based on pre-trained linguistic models to identify relevant information, and a computed answer is sent back to the robot. Depending on the task, it might be necessary to incorporate other involved providers to receive additional required information and access. The raw data itself might be used to improve the analysis techniques and results of the model. Thereby, risk identification does not only concentrate on the protection of data against theft but also on the protection against misuse on the side of all involved companies and providers [29]. As an example, the user asks the robot to turn on the music. The voice command is transferred to the companies data centers. After processing and analysis, the command is transmitted to affiliated services, e.g., streaming services to turn on the music.[1]

Typically, this step contrasts the different implementation techniques, and at the end, a final decision needs to be selected. The use case does not incorporate many sensors, but the robot's capabilities entail potential risks. Therefore, the risk of network connectivity is necessary to highlight the importance of maintaining, storing, and receiving relevant information for the interaction. Concomitantly, involved providers and third parties need to be investigated as they all represent potential threats. The next step deals with an analysis of requirements for protection to achieve a privacy level that is suitable and appropriate.

4.2 Risk analysis

Risk analysis is conducted parallel to the design thinking process phases of *define* and *ideate*. Within these two steps, the context and the features need to be concretized to focus the development. For this use case, this implies two aspects. First, it has to be determined how the identified features shall be implemented to which extent and sensors are necessary. Second, the specific use case scenario needs to be specified. Those two aspects are important because the use case scenario determines

1 Authorization code flow between the application services, proposed by Spotify as exemplary streaming service https://developer.spotify.com/documentation/general/guides/authorization-guide/

which protection goals are most relevant. The following example refers to two use case scenarios, (1) entertainment purpose and (2) health care purpose, to demonstrate the differences.

Risk analysis is then used to ensure privacy requirements and choose suitable measurements and related technologies. It concentrates on analyzing the protection goals based on the identified risks and sensitivity of the information. As already pointed out in Section 3.2, not all protection goals can be realized to the same level [35]. Therefore, a prioritization of protection goals needs to be evaluated for every use case scenario.

4.2.1 Use case scenario: Entertainment robot

Seeing the robot as an **entertainment device** for the users, the prioritized goals would be *intervenability* and *transparency*. As described earlier, the more features the robot incorporates, the more potential risks might occur. Transparency gives users the inside view of which functions access and process which information, what data are recorded, and when and for what purpose it is used. This inside view becomes specifically important in terms of awareness and self-determination. Thereby, it needs to be visible for the user which data are collected, where it is processed, and the purpose of processing. The ability of music streaming needs a record of analyzed data and the authorization to forward the data to the incorporated service. Furthermore, it needs to be made clear which sensors are used and that, e.g., music streaming does not request access to the camera or other information necessary for other services. Such links indicate that it needs to be visible which services are integrated and which services use which sensors.

Transparency serves as a basis for intervenability and enables the user to make decisions about functionalities themselves. Intervenability might allow users to decide on their own which features are enabled or disabled. Ideally, they can also choose when the robot and its features are permitted to use the microphone or the camera. Thereby, switching off the camera should not lead to a full loss of functionality. Depending on the user's decision, there is the need for several functional levels. It might be possible that a robot possesses a camera and a microphone. Still, the users do not want the robot to identify them through face recognition and disables the camera. It should still be able to interact with the robot via microphone but with limited capabilities. So far, robots must be connected to the Internet and must have enabled all sensors. Otherwise, most of the robot's features cannot work as they do not have access to any data or information. The aspect of functionality needs to be made more individualized.

As a third aspect, *availability* is prioritized above confidentiality, as interaction is based on fast response rates, and interaction needs to be fluent. The robot must be capable of reacting immediately, be it linguistically or gesturally. In addition, features such as reminders or timers are time dependent and should be reliable.

4.2.2 Use case scenario: Health care robot

Time dependence becomes even more important when discussing the use case scenario of a health care robot. *Availability* can be seen as the most relevant protection goal as time can play a decisive factor. Time-relevant features imply medication reminders as well as emergency monitoring and the potential need to call for help.

Similar to the use case scenario before, *transparency* is a relevant factor. The implication for the importance slightly differs. In this use case scenario, transparency is relevant to keep the overview. It affects authorization and authentication mechanisms as well as the listing of certain reminders or other health conditions.

Transparency is accompanied by the third protection goal of *integrity*. For the health care robot, the primary aim is to protect the user's data, ensure the correctness of the data, and protect the health condition. If the robot provides a reminder for, e.g., medication, it needs to be guaranteed that nothing could be manipulated, e.g., that reminders do not occur too often or reminds to take the wrong medicine. There needs to be a guarantee concerning the correctness of provided information. Intervention should only be possible minimally, and as the robot is meant to monitor the user, sensors are not allowed to be easily switched off. Pillo, as an example, is a robot health companion with included medicine cabinets and user recognition to provide the correct medication. This feature needs to ensure a 100%, which the user has identified correctly and that someone without permission can replace medication or change the timer.[2]

4.3 Risk mitigation

Risk mitigation takes place within the *prototyping* phase. The user can test several implementation techniques from

2 Pillo health companion: https://pillohealth.com/

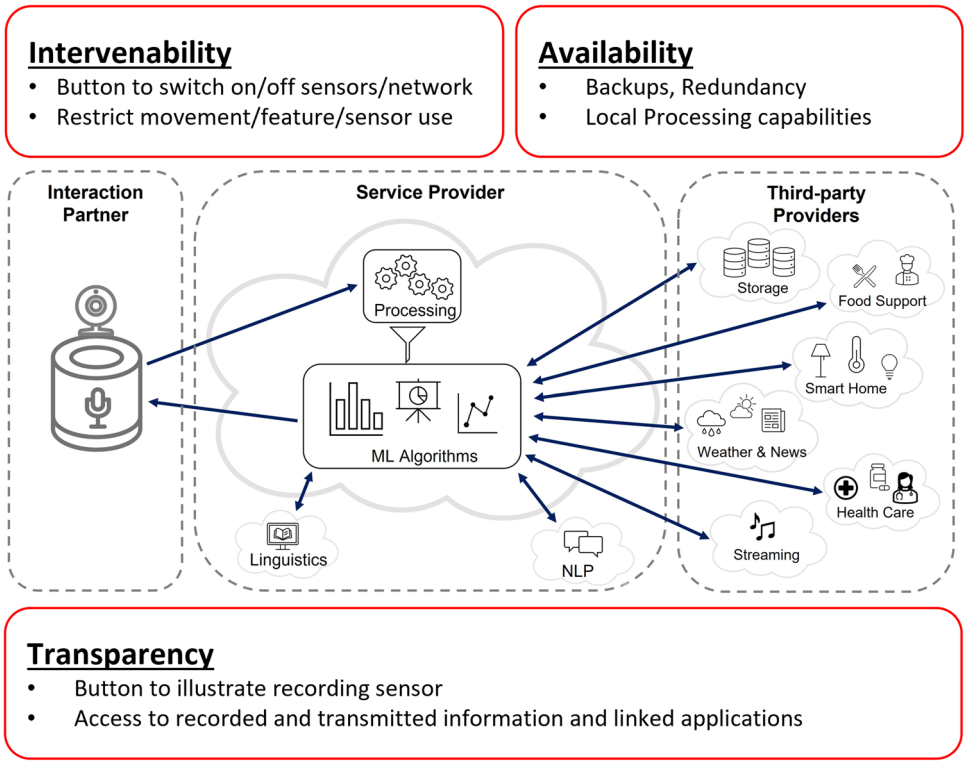

Figure 4: Mitigation strategies for respective interrelations in the context of health care supervision or work support.

the user for the specific use case scenarios. This involvement gives future users the chance to participate in the design decision and thereby create an intuitively operable robot and modifiable according to one's preferences.

Availability is a relevant goal for an interactive robot, and both use case scenarios. Measures to ensure availability provided by the SDM[3] are, e.g., data backups, redundancy of hard- and software components, repair strategies, alternative processes, and protection against external influences. These measures would have to be carried out by the relevant service providers (Figures 4 and 5). Availability needs to be ensured for all involved service providers. It needs to be checked that all service providers fulfill the availability requirements and that the measures of the involved stakeholders are also compliant with the requirements and the principles of user protection. Even though availability is considered of higher importance, *confidentiality* needs to be ensured as well. To ensure *confidentiality*, measures such as authentication, encryption, and authorization proved to be useful concepts to prevent others from gaining access to personal data [22].

For *transparency* as the second relevant protection goal for both use case scenarios, the most relevant aspect deals with the robot's feature of recording. It needs to be visible for the user when the robot is recording. A flashing can realize this LED, indicating a recording microphone. Furthermore, an essential component for transparency concentrates on the transparency of data flows. It should be visible and understandable for the user, how and which information is transferred, used, and stored, especially when third parties are involved in integrating more features (Figure 3). If certain features are not available, it should still be possible to inform the user about these issues. In the context of the second use case, transparency also becomes important in terms of data tracking. It needs to be comprehensible which health care status information is forwarded to the medical app or the doctor or how specific work processes were chosen and carried out. *Unlinkability* should be ensured in a way that the integrated services do not communicate and exchange data among each other when not necessary.

Integrity and *intervenability* are assigned two different levels of importance within the two use case scenarios. *Intervenability* is seen as more relevant and important within the use case of an entertainment robot (Figure 5). Preferably, this would lead to mitigation strategies where the user can decide the "working principle" of the robot. Beyond a status LED, a button helps to turn on/off the microphone or the camera. In addition, a privacy dashboard where information of activities is listed transparently

3 https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V2.0b.pdf

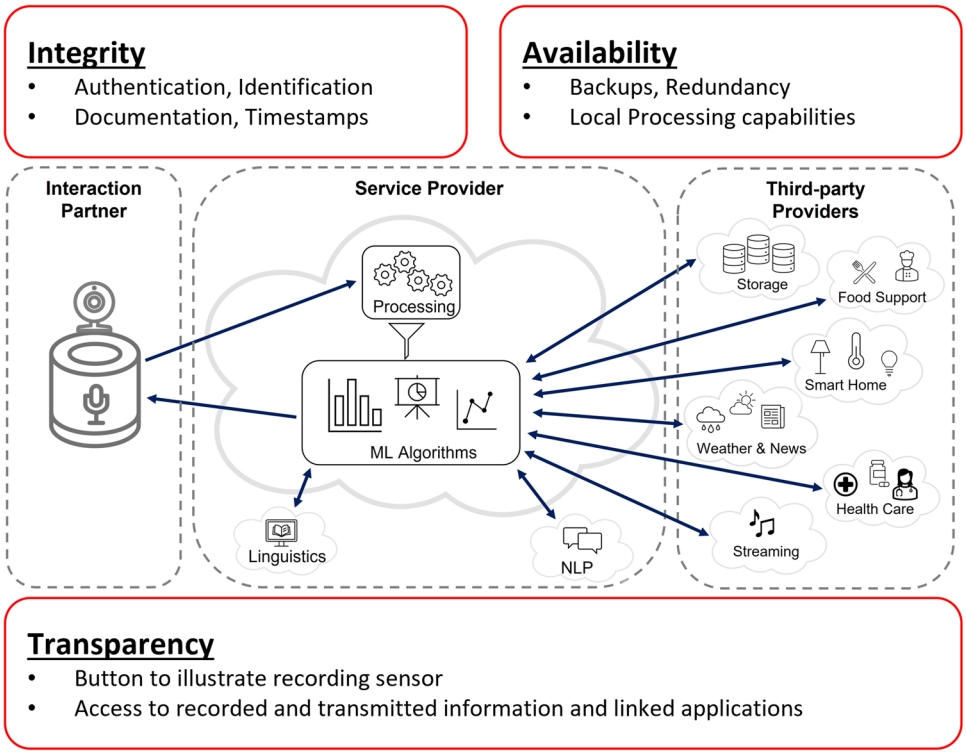

Figure 5: Mitigation strategies for respective interrelations in the context of entertainment.

needs to allow unlinking or disabling certain features that are not required or wanted.

In the health care scenario, *integrity* is more relevant as, e.g., emergency processes or medication reminders should not be modifiable in an easy way. Modifications should be allowed only using authentication techniques, as changes could cause harm and damage if done improperly without permission. In the case of the second use case scenario, where the camera plays an important role in monitoring the users and their activities, it might be a useful measure to use image filter techniques just to analyze the relevant aspects of the data. Several manipulation techniques can be applied to concentrate on the essential content, e.g. blurring, sketching, or redaction [39–41].

Furthermore, context awareness can not only be discussed depending on the intended use case scenario. Context-awareness is additionally part of robot's behavior. For the entertainment use case scenario, this would require that the robot only listen and record when and where it is allowed to, and the user allows it. For example, video recording within the bathroom and bedroom should be prohibited by default to safeguard privacy. The microphone should only record when the user speaks to the robot. To control this, three different listening principles for smart speakers exist so far, divided into *manually activated*, *speech activated*, and *always on* [42]. The *always-on* solution should be avoided for this use case scenario. Users should rather be able to determine when to start a conversation, for example, by pressing a button with the help of keywords or using a gesture recognizable via camera.

For the second use case scenario, switching off the camera should not be possible as it is used for emergency monitoring. Nevertheless, as an emergency might also occur within a bathroom or bedroom, the user needs to make clear to the robot to not record over a while, e.g., when having a shower. Emergency monitoring while not using the camera can be realized with a question, and the user has to answer.

Overall, the way of intervenability needs to be determined together with the user. By pressing a button or using a regulator, the user can switch on or off specific sensors. Still, it can also be realized using an interface for the robot that is manipulable via a touchpad or voice commands. There is no specific available solution. Therefore, it is of utmost importance to propose various solutions to decide together with the user.

5 Discussion and conclusion

This use case proposed the relevance of risk assessment, especially for security and privacy protection. In the scenario of an interactive robot that should be seen as a

companion, the topic of trust, honesty, and reliability are of utter importance [43] as the robot will receive a lot of very personal and sensitive information. This feeling of companionship sounds illusory, as a robot is a technical device developed for commercial purposes. The use case referred to the robot as a companion, which in our opinion sounds misleading. Of course, it is intended to trust the robot to some extent. Otherwise, a user will not use the robot at all with accompanied functionality. Nevertheless, we should be aware of interacting with a robot and not with a human friend. Moreover, it is a device that pretends to be our friend, but the manufacturers behind it are in charge of all the user's data. Therefore, it becomes even more important to raise users' awareness toward protection in certain situations.

The privacy framework consists of risk identification, risk analysis, and risk mitigation functions as guiding help. It presents the relevant issues that need to be investigated for a privacy-respecting development. It is not only about risks that are accompanied by certain installed sensors. Furthermore, it is not only about the investigation of potential external threats and thefts initiated by hackers. In contrast to the concept of "*judicious sensor selection*" of Eick and Anton [24], this use case could show that the risks do only partly arise with the use of high-risk sensors, for instance, cameras [21]. Rather, it is about the overall and holistic protection of personal and sensitive information against theft and misuse on the side of the involved service providers. Risk-afflicted issues occur with the installation of an internet connection. A robot companion does not necessarily need to be equipped with many sensors. Being equipped with microphones does already entail a collection of information that can be highly sensitive. In robotics research so far, this issue involves the considerations of (cyber-)security protection. Privacy protection is equally important and has become a highly relevant topic with robots in domestic environments and private spaces.

The privacy framework was introduced as a practice-oriented approach to enhance the PbD concept. The privacy risk assessment covers five principles of the PbD concept. It involves the proactive view on data protection (1), data protection by default (2), the embedding into the design process (3), the visibility and transparency (6), and principle (7) when the user is involved. The accomplishment of the full functionality and a win–win development for principle (4) can only be successful when all stakeholders, specifically the users, participate in giving input. The end-to-end cycle protection (5) can only be covered by information protection within all involved service providers. All of them are obliged to carry out such a risk assessment to achieve this principle. Overall, the proposed concept offers a first approach for privacy-respecting development.

Thereby, it is emphasized that the user must be involved throughout the entire development process. Even though this was not the focus of this article, user participation is important. Only the user can provide an insight view and give constructive feedback on putting things into practice. Another advantage of user participation is the contribution of potentially unconventional ideas towards robot development and certain implementation techniques. Concerning privacy, the proposed methodologies can also be used in user participation as they are easy to apply. In addition, the user knows about privacy and security issues and potential risks and can be aware of them. Such awareness enables users to get confronted with the topic of privacy for sensitization. Furthermore, the chance to co-determine gives users a new perspective toward robots, resulting in positive effects toward trust and companionship.

Funding information: This work was supported by the Ministry for Science and Culture of Lower Saxony as part of the program "Gendered Configurations of Humans and Machines (KoMMa.G)."

Conflict of interest: Authors state no conflict of interest.

Informed consent: Informed consent was obtained from all individuals included in this study.

Data availability statement: The datasets generated during and/or analyzed during the current study are available from the corresponding author on reasonable request.

References

[1] International Federation of Robotics, "Executive summary world robotics 2019 service robots," 2019. [Online]. Available: https://ifr.org/downloads/press2018/executive_summary_wr_service_robots_2019.pdf.

[2] C.-A. Smarr, T. L. Mitzner, J. M. Beer, A. Prakash, T. L. Chen, et al., "Domestic robots for older adults: attitudes, preferences, and potential," *Int. J. Soc. Robot.*, vol. 6, no. 2, pp. 229–247, 2014, DOI: https://doi.org/10.1007/s12369-013-0220-0.

[3] D. S. Syrdal, K. Dautenhahn, K. L. Koay, and W. C. Ho, "Views from within a narrative: Evaluating long-term human–robot interaction in a naturalistic environment using open-ended scenarios," *Cognit. Comput.*, vol. 6, no. 4, pp. 741–759, 2014, DOI: https://doi.org/10.1007/s12559-014-9284-x.

[4] E. M. Albina and A. A. Hernandez, "Assessment of the elderly on perceived needs, benefits and barriers: Inputs for the

design of intelligent assistive technology," in: *2018 16th International Conference on ICT and Knowledge Engineering* (*ICT&KE*), Bangok, Thailand: IEEE, 2018, pp. 1–10, DOI: https://doi.org/10.1109/ICTKE.2018.8612447.

[5] C. Bartneck, T. Belpaeme, F. Eyssel, T. Kanda, M. Keijsers, and S. Šabanović, *Human–Robot Interaction: An Introduction*, Cambridge: Cambridge University Press, 2020.

[6] S. Frennert and B. Östlund, "Seven matters of concern of social robots and older people," *Int. J. Soc. Robot.*, vol. 6, no. 2, pp. 299–310, 2014, DOI: https://doi.org/10.1007/s12369-013-0225-8.

[7] I. Leite and J. F. Lehman, "The robot who knew too much: Toward understanding the privacy/personalization trade-off in child-robot conversation," in *Proceedings of the 15th International Conference on Interaction Design and Children*, 2016, pp. 379–387, DOI: https://doi.org/10.1145/2930674.2930687.

[8] M. Nagenborg, R. Capurro, J. Weber, and C. Pingel, "Ethical regulations on robotics in Europe," *AI Soc.*, vol. 22, no. 3, pp. 349–366, 2008, DOI: https://doi.org/10.1007/s00146-007-0153-y.

[9] B. C. Stahl and M. Coeckelbergh, "Ethics of healthcare robotics: Towards responsible research and innovation," *Robot. Autonom. Syst.*, vol. 86, pp. 152–161, 2016, DOI: https://doi.org/10.1016/j.robot.2016.08.018.

[10] D. Feil-Seifer and M. J. Matarić, "Socially assistive robotics," *IEEE Robot. Autom. Magazine*, vol. 18, no. 1, pp. 24–31, 2011, DOI: https://doi.org/10.1109/MRA.2010.940150.

[11] A. Sharkey and N. Sharkey, "Granny and the robots: ethical issues in robot care for the elderly," *Ethics Inform. Technol.*, vol. 14, no. 1, pp. 27–40, 2012, DOI: https://doi.org/10.1007/s10676-010-9234-6.

[12] S. Sami, Y. Dai, S. R. X. Tan, N. Roy, and J. Han, "Spying with your robot vacuum cleaner: eavesdropping via lidar sensors," in *Proceedings of the 18th Conference on Embedded Networked Sensor Systems*, 2020, pp. 354–367, DOI: https://doi.org/10.1145/3384419.3430781.

[13] F. E. Fernandes, G. Yang, H. M. Do, and W. Sheng, "Detection of privacy-sensitive situations for social robots in smart homes," in *2016 IEEE International Conference on Automation Science and Engineering* (*CASE*), Fort Worth, TX, USA: IEEE, 2016, pp. 727–732, DOI: https://doi.org/10.1109/COASE.2016.7743474.

[14] M. Astor, "Your roomba may be mapping your home, collecting data that could be shared," *The New York Times*, vol. 25, 2017.

[15] D. J. Solove, *The Digital Person: Technology and Privacy in the Information Age*, New York: NYU Press, vol. 1, 2004.

[16] "Regulation (EU) 2016/679 of the European parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (General Data Protection Regulation)," pp. 1–88, 2017.

[17] R. Leenes, E. Palmerini, B.-J. Koops, A. Bertolini, P. Salvini, and F. Lucivero, "Regulatory challenges of robotics: some guidelines for addressing legal and ethical issues," *Law Innovat. Technol.*, vol. 9, no. 1, pp. 1–44, 2017, DOI: https://doi.org/10.1080/17579961.2017.1304921.

[18] C. Lutz and A. Tamò, "RoboCode-Ethicists: Privacy-friendly robots, an ethical responsibility of engineers?," in *Proceedings of the ACM Web Science Conference*, 2015, art. 21, DOI: https://doi.org/10.1145/2786451.2786465.

[19] A. Cavoukian, "Privacy by design: The 7 foundational principles," DOI: https://privacy.ucsc.edu/resources/privacy-by-design—foundational-principles.pdf.

[20] T. Denning, C. Matuszek, K. Koscher, J. R. Smith, and T. Kohno, "A spotlight on security and privacy risks with future household robots: attacks and lessons," in *Proceedings of the 11th International Conference on Ubiquitous Computing*, Orlando, Florida: ACM, 2009, pp. 105–114, DOI: https://doi.org/10.1145/1620545.1620564.

[21] F. J. R. Lera, C. F. Llamas, Á. M. Guerrero, and V. M. Olivera, "Cybersecurity of robotics and autonomous systems: Privacy and safety," in *Robotics-Legal, Ethical and Socioeconomic Impacts*, InTech, 2017, DOI: https://doi.org/10.5772/InTechopen.69796.

[22] C. Cerrudo and L. Apa, *Hacking Robots Before Skynet*, IOActive Website, 2017.

[23] T. Heuer, I. Schiering, and R. Gerndt, "Privacy-centered design for social robots," *Interact. Stud.*, vol. 20, no. 3, pp. 509–529, 2019, DOI: https://doi.org/10.1075/is.18063.heu.

[24] S. Eick and A. I. Anton, "Enhancing privacy in robotics via judicious sensor selection," in *Proceedings – IEEE International Conference on Robotics and Automation*, 2020, pp. 7156–7165, DOI: https://doi.org/10.1109/ICRA40945.2020.9196983.

[25] M. Rueben, A. M. Aroyo, C. Lutz, J. Schmölz, P. Van Cleynenbreugel, et al., "Themes and research directions in privacy-sensitive robotics," in *2018 IEEE Workshop on Advanced Robotics and Its Social Impacts* (*ARSO*), Genova, Italy: IEEE, 2018, pp. 77–84, DOI: https://doi.org/10.1109/ARSO.2018.8625758.

[26] S. Spiekermann, "The challenges of privacy by design," *Commun. ACM*, vol. 55, no. 7, pp. 38–40, 2012, DOI: https://doi.org/10.1145/2209249.2209263.

[27] M. Alshammari and A. Simpson, "Towards a principled approach for engineering privacy by design," in *Privacy Technologies and Policy, APF 2017, Lecture Notes in Computer Science, vol. 10518*, Cham: Springer, 2017, pp. 161–177, DOI: https://doi.org/10.1007/978-3-319-67280-9_9.

[28] U. Pagallo, "Robots in the cloud with privacy: A new threat to data protection?," *Comput. Law Secur. Rev.*, vol. 29, no. 5, pp. 501–508, 2013.

[29] I. Schiering, B. A. Mester, M. Friedewald, N. Martin, and D. Hallinan, "Datenschutz-risiken partizipativ identifizieren und analysieren," *Datenschutz und Datensicherheit-DuD*, vol. 44, no. 3, pp. 161–165, 2020, DOI: https://doi.org/10.1007/s11623-020-1243-y.

[30] C. D. Raab, "Information privacy, impact assessment, and the place of ethics," *Comput. Law Secur. Rev.*, vol. 37, art. 105404, 2020, DOI: https://doi.org/10.1016/j.clsr.2020.105404.

[31] N. Martin, M. Friedewald, I. Schiering, B. A. Mester, D. Hallinan, and M. Jensen, *The Data Protection Impact Assessment According to Article 35 GDPR. A Practitioner's Manual*, Stuttgart: Fraunhofer Verlag, 2020. DOI: https://publica.fraunhofer.de/eprints/urn_nbn_de_0011-n-5900152.pdf.

[32] H. Plattner, C. Meinel, and U. Weinberg, *Design-thinking*, Berlin, Heidelberg: Springer, 2009.

[33] R. L. Finn, D. Wright, and M. Friedewald, "Seven types of privacy," in *European Data Protection: Coming of Age*, Dordrecht: Springer, 2013, pp. 3–32, DOI: https://doi.org/10.1007/978-94-007-5170-5_1.

[34] A. Bhardwaj, V. Avasthi, and S. Goundar, "Cyber security attacks on robotic platforms," *Netw. Secur.*, vol. 2019, no. 10, pp. 13–19, 2019, DOI: https://doi.org/10.1016/S1353-4858(19)30122-9.

[35] M. Hansen, M. Jensen, and M. Rost, "Protection goals for privacy engineering," in *Security and Privacy Workshops* (*SPW*), *2015 IEEE*, San Jose, CA, USA: IEEE, 2015, pp. 159–166, DOI: https://doi.org/10.1109/SPW.2015.13.

[36] S. Yong, D. Lindskog, R. Ruhl, and P. Zavarsky, "Risk mitigation strategies for mobile wi-fi robot toys from online pedophiles," in *2011 IEEE Third International Conference on Privacy, Security, Risk and Trust* (*PASSAT*) *and 2011 IEEE Third International Conference on Social Computing* (*SocialCom*), Boston, MA, USA: IEEE, 2011, pp. 1220–1223, DOI: https://doi.org/10.1109/PASSAT/SocialCom.2011.194.

[37] T. Heuer, I. Schiering, and R. Gerndt, "Me and my robot-sharing information with a new friend," in *IFIP International Summer School on Privacy and Identity Management*, Vienna, Austria: Springer, 2018, pp. 189–204.

[38] C. Pearl, *Designing Voice User Interfaces: Principles of Conversational Experiences*, Gravenstein, CA: O'Reilly Media, Inc., 2016.

[39] J. Schiff, M. Meingast, D. K. Mulligan, S. Sastry, and K. Goldberg, "Respectful cameras: Detecting visual markers in real-time to address privacy concerns," in *Protecting Privacy in Video Surveillance*, London: Springer, 2009, pp. 65–89.

[40] A. Hubers, E. Andrulis, W. D. Smart, L. Scott, T. Stirrat, et al., "Video manipulation techniques for the protection of privacy in remote presence systems, in *Proceedings of the Tenth Annual ACM/IEEE International Conference on Human-Robot Interaction Extended Abstracts – HRI'15 Extended Abstracts*, pp. 59–60, 2015, DOI: https://doi.org/10.1145/2701973.2702048.

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

[42] S. Gray, "Always on: privacy implications of microphone-enabled devices," in *Future of Privacy Forum*, Washington, DC, 2016.

[43] K. Dautenhahn, S. Woods, C. Kaouri, M. L. Walters, K. L. Koay, and I. Werry, "What is a robot companion – friend, assistant or butler?," in *2005 IEEE/RSJ International Conference on Intelligent Robots and Systems*, Edmonton, AB, Canada: IEEE, 2005, pp. 1192–1197, DOI: https://doi.org/10.1109/IROS.2005.1545189.