Me and My Robot - Sharing Information with a New Friend

Tanja Heuer, Ina Schiering, Reinhard Gerndt

▶ **To cite this version:**

Tanja Heuer, Ina Schiering, Reinhard Gerndt. Me and My Robot - Sharing Information with a New Friend. Eleni Kosta; Jo Pierson; Daniel Slamanig; Simone Fischer-Hübner; Stephan Krenn. Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data : 13th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Vienna, Austria, August 20-24, 2018, Revised Selected Papers, AICT-547, Springer International Publishing, pp.189-204, 2019, IFIP Advances in Information and Communication Technology, 978-3-030-16743-1. 10.1007/978-3-030-16744-8_13 . hal-02271664

HAL Id: hal-02271664

https://inria.hal.science/hal-02271664

Submitted on 27 Aug 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

Me and My Robot - Sharing Information with a New Friend

Tanja Heuer, Ina Schiering and Reinhard Gerndt

Ostfalia University of Applied Sciences
Wolfenbüttel, Germany
{ta.heuer, i.schiering, r.gerndt}@ostfalia.de

Abstract. This paper investigates user perception regarding social robots and personal information disclosure. During a study two participant groups stated their attitude towards functionality, shared personal information and the interest of transparency and intervenability. The impact of technical background knowledge regarding users attitude and perception was examined. Participants working with robots have a more open-minded attitude to share personal information achieving a wider range of functionality. Both groups care about transparency of collected data and the possibility of intervenability.

Keywords: social robot, HRI, Human-Robot Interaction, privacy

1 Introduction

Since Amazon Echo, Google Home and iRobot Roomba are already part of daily life, Asus Zenbo is the next generation robot entering homes. Although the current focus on social robots is on care and most studies are conducted with older people or children with chronic impairments [15], the features of social robots are not only addressing *people in need of care*, but everyone who wants to have support and assistance at home or a hand's free way to read news or listening to music when, e.g. the phone is not within reach. To contribute assistance, it communicates with other smart devices, informs about news and appointments, supports music streaming, helps cooking and supervises the health care status. To assist in all these areas, robots make use of sensors like cameras or microphones. To show itself as assistant and companion, the robot collects a huge amount of personal data to be able to simulate a natural interaction. This collected data is often processed using cloud services to allow a fast response and reaction time on requests.

Using smart home technologies and devices leads to a variety of possible privacy risks. With a microphone there is a risk of eavesdropping. A camera increases the risk of spying. Cloud service connections enable unauthorized access to personal data shared with the devices. With every additional sensory input a list of new hazards appear. It is important to make users aware of potentially risks and of the implication of disclosing personal information. To achieve this

awareness, users need to know which data is required for specific features and for what purposes the data is processed.

To investigate users preferences regarding functionality and shared personal information, a questionnaire is conducted as a first step. Furthermore it should be examined, if users are interested in the operating principles of robots to get an idea how and for what purposes personal information is processed. Even though, a questionnaire is not as representative as conducting user studies because of effects as the privacy paradox - sharing attitude and sharing behavior [10], the aim is to get a predication of younger people's attitude towards social robots and how technical background knowledge affects the way of thinking regarding robot expectations. In a second step, the correlation between features and personal information is investigated. The importance of transparency in the context of this relation needs to be outlined unambiguously.

2 Background Social Robots

We are facing a world of smart homes and connected things. Amazon Echo and Google Home are already part of it and this constitutes several risks. In May 2018, Amazon Echo recorded a private conversation and transferred that to a friend. Thereupon, Amazon argued that there were bad circumstances. Already in 2017, it was determined that a previous version of Google Home was permanently eavesdropping its users. The information was then transferred to a Google server although the Google Home device only should react on *Ok, Google*.

As Amazon Echo and Google Home, also other robots are integrated into the smart home. The vacuum cleaning robot (Roomba980 [1]) can be started via Alexa Echo, saying "Alexa, ask Roomba to start cleaning."[1] or via Google Home saying "Ok Google, tell Roomba to start cleaning"[2]. Figure 1 shows the example scenario using a smart home vacuum cleaning robots. With the help of a camera and a laser range scanner it maps the home and processes information like cleaned and non cleaned areas. Initially, this feature was developed for intelligent cleaning service of the robot and it was processed on the robot and no one had access to that. With an update, iRobot decided to offer a new feature and revealed this map in an application where users are able see the robots status and by default everything is sent to the iRobot Cloud[3]. Furthermore, it was already discussed if this data could be sold to third parties like Amazon or Google because they are cooperating anyway [4].

[1] https://homesupport.irobot.com/app/answers/detail/a_id/1412//˜/compatible-commands-for-a-wi-fi-connected-roomba-and-alexa.

[2] https://homesupport.irobot.com/app/answers/detail/a_id/1509/˜/compatible-commands-for-a-wi-fi-connected-roomba-and-the-google-assistant

[3] http://desupport.irobot.com/app/answers/detail/a_id/1406/˜/clean-map%E2%84%A2-report-data-and-the-irobot-cloud.

[4] https://www.theguardian.com/technology/2017/jul/25/roomba-maker-could-share-maps-users-homes-google-amazon-apple-irobot-robot-vacuum

Fig. 1. Smart vacuum cleaning using the Roomba980

A more complex robot for home use is Zenbo, developed by Asus [5]. This robot is marketed with a wide range of functionalities. On the one hand, it is able to remind of medication or meetings, sends notifications to family members in case of emergency and controls other smart devices in the home. On the other hand, it supports online activities like shopping, music and video streaming and searches for recipes. To allow also special functions as e.g. healthcare checks, a broad variety of personal data needs to be collected and the robot needs to be connected to the internet all the time. The collected information includes voice, video and communication records[6] but it is not mentioned explicitly, how privacy and security of this information is ensured.

3 Related Work

As already mentioned, the research of social robots is often linked to the healthcare sector. In many different ways, older people are increasingly integrated into the development process of robots for assistive tasks. As one method, surveys and interviews are conducted to ask about user preferences. Various studies investigated the attitude of people towards robots and in which situations robots or human assistance is preferred [20, 23, 19, 16].

Apart from design and features, some studies dealt with the topic of privacy and possible concerns of users towards social robots. Syrdal et al.[21] focused on data storage and which data users would agree with to be stored. Caine et al. [6] investigated changing behavior of older people when they were recorded. Concerning privacy, more studies focused on the identification of general privacy risks [17, 11] or considered privacy concerns in a more general smart home context [24, 7]. Aroyo et al. [4] investigated the disclosure of personal information when participants started to trust a robot. Because of smart home systems communicating with the robots (see Figure 1), it is also worth to take a look at topics investigated in this area. For the healthcare sector, there are smart home solutions [22] and smartphone applications [8] where it is investigated which personal data participants are willing to disclose. More general privacy issues using

[5] https://benchmarkreviews.com/41895/asus-zenbo-robot-announced/
[6] https://www.asus.com/Terms_of_Use_Notice_Privacy_Policy/Privacy_Policy

smart home systems are analysed in the context of data tracking and activity monitoring [12, 18, 14, 5].

4 Research Approach

The aim of this survey was to evaluate younger people's technical background knowledge and how this might affect the perception and use of social robots. In doing so, the focus is on privacy concerns because they have a negative implication on the usage of robots [2]. Therefore this influencing determinant needs to be investigated further. Next to preferred features, participants should state their willingness to disclose several personal information.

One the one hand, we want to investigate whether potential users are aware of the connection between use of features and provision of personal information. On the other hand, we want to know if in general users are interested in transparency of the operating principles of a robot, how and which personal data is processed and for what purpose it is used. Because we assume that the interest in transparency and the awareness is related to technical know-how, we investigated two user groups.

5 Methodology

5.1 Questionnaire

Before handing in the survey, participants had to give their informed consent. They were informed about the research topic of the survey and how the collected data will be handled. All collected information is stored anonymously and encrypted and will not be given to third parties.

The questionnaire was conducted on paper. It is arranged in three major sections. The first part determines favored features for a robot. Participants had the ability to choose between different features and second, they could describe additional, not mentioned features. Furthermore, they should state their attitude towards usage of robots by more than one person and if the robot should be able to distinguish between people. The second section asked for preferences according to collected data. Participants should decide what personal information the robot is allowed to collect.

In a third step, the interest of intervention towards data collection and processing should be stated (scale from -2=strongly disagree to 2=strongly agree). Partly, the questions are adapted from the UTAUT model [3] and a study investigating preferences of older adults [23]. In the last section, users were asked for demographical information of participants as age, sex, education, technical affinity and technical devices which are used regularly.[7]

[7] The whole questionnaire can be downloaded under the following link: https://powerfolder.sonia.de/getlink/fiZbw6TM9E8Vb2aCM6DyEor/Questionnaire_IFIP2018.pdf

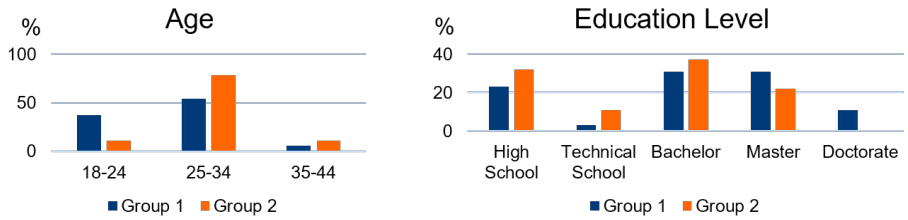

Fig. 2. Age and graduation distribution of both groups

5.2 Participants

In total, quantitative data from 73 participants was collected. Participants for *group 1* were chosen randomly during the RoboCup competition 2018 in Montreal, Canada. Participants for *group 2* were chosen randomly during a social event in Germany also in 2018.

Group 1 consisted of 35 participants - 7 female, 25 male and 3 non-disclosed participants. The age and level of degree of both groups is opposed in 2.37.1% were in the range of 18-24 years, 54.3% were in the range of 25-34 years. The most completed educational qualification in *participant group 1* are Bachelor's degree (31,4%) and Master's degree (31,4%). 22.9% had a high school degree. 68.6% had a student status, 25.7% are working full time. Smartphones (100%) and laptops (97%) are daily used technical devices. Game consoles are regularly used by 28.6% of the respondents, a vacuum cleaning robot by 22,8% of the participants, Alexa Echo and Google Home by only 14.3%.

Group 2 consisted of 38 participants - 16 female, 18 male and 4 non-disclosed participants. 79% were in the range of 25-34 years. The two highest qualification degrees are Bachelor degree (36.8%) and high school degree (31.6%). 63.2% are employed full time, the rest of the respondents were students. Smartphones (100%) and laptops (94.7%) are daily used technical devices. Games consoles and vacuum cleaning robots are regularly used by 15.8% of the participants, Alexa Echo and Google Home by only 10.5%.

Figure 2 illustrates the age distribution and the educational level of both groups.

Additionally, participants were asked to rate their self-evaluation of technical affinity (scale from -2=strongly disagree to 2=strongly agree):

1. *easy usage*: It would be easy for me using a robot at home
2. *easy learning*: Learning how to use a home robot would be easy for me.
3. *willingness of usage*: I am willing to use technical devices.
4. *usage is fun*: I have fun using technical devices.
5. *problem solving*: I am able to solve technical problems on my own.

Figure 3 shows the average of level of agreement for technical affinity. For all statements, *group 1* states a higher level of agreement than *group 2*. Whereas the average level of agreement is between 1.3 (easy usage) and 1.8 (willingness of

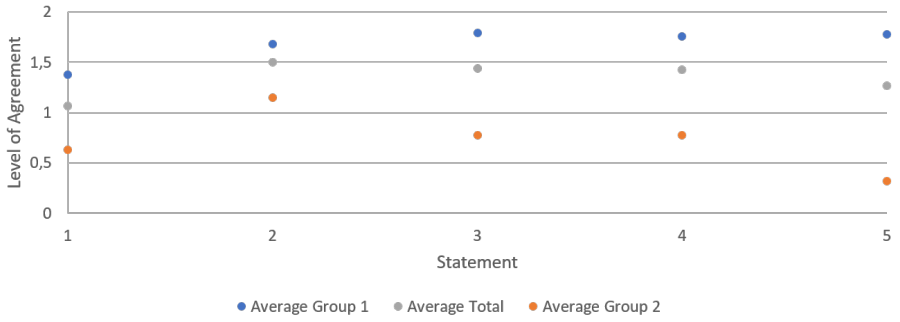

Fig. 3. Technical Affinity of Participant groups in average

usage) for *group 1*, *group 2* only reaches an average level of agreement between 0.3 (problem solving) and 1.2 (easy learning).

6 Results

6.1 Functionality of a Robot

The first part of the questionnaire adressed applications of the robot. Respondents could select as many features as they like and in a second step add their own ideas of features a robot needs to have. The chosen features are already part of various social robots. As a sthird part of this category, participants should state, if a robot should be used by more than one person and if it should able to distinguish the users. Prescribed possibilities of features are the following:

- The robot reminds me when to take my medicine.
- The robot keeps an eye on me, possibly calls for rescue.
- The robot takes over cleaning activities.
- The robot keeps me company.
- The robot moves autonomously.
- The robot provides cognitive exercises.
- The robot interfaces with other technologies in my home.
- I can cuddle and hug my robot.
- I video conference with my friends and family via the robot.
- Friends and family can monitor in case of problems.

As a result, the radar chart (see Figure 4) shows the percentual answers of every feature. It can be seen that both groups have the same peaks. The most chosen features are cleaning assistance, autonomously moving, communication with other technologies in home and video conferencing with other people. But only for cleaning assistance, both groups show the same high interest (>90%). For all other features, approximately one third less of *group 2* wanted to have

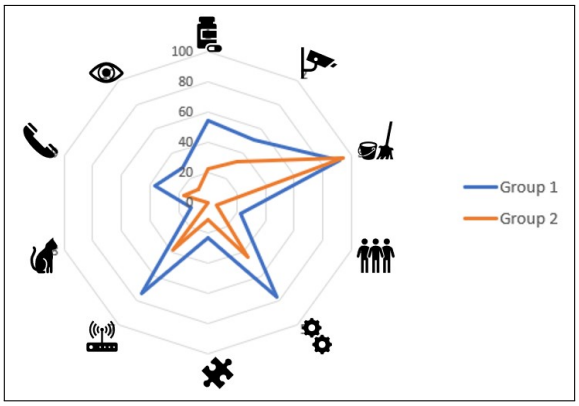

Fig. 4. Possible selectable features for the robot

these features. Reminder for medication and surveillance in case of emergency are also two interesting features for half of *group 1*.

In a second step, participants were able to state their own ideas. 77% of the participants of *group 1* wrote down their own ideas or specified tasks, in *Group 2* only 50% did. *Group 1* listed specific tasks for cleaning activities like dish washing, floor cleaning, clearing away things, laundry and take out garbage. Additionally, the robot shall be able to cook or help cooking (20%), it shall have the same features as Alexa Echo or Google Home (11%), can remind you of things (11%) and it shall be part of home security - surveillance in case of emergency when no one is at home(11%). In *group 2* the most popular answer was vacuum cleaning. Other answers of *group 2* were a reminder function (11%) and security issues (11%).

It is accepted by 85% of *group 1* and 100% of *group 2* that the robot can be used by everyone at home. The distinction of people at home is important for 92% of *group 1* but only for 60% of *group 2*.

6.2 Disclosed Information

Participants selected personal data they are comfortable with sharing it. The right radar chart (see Figure 5) shows the answers. *Group 1* is more willing to share personal information with the robot. More than 60% allow the robot to know personal information like name, age and sex but also grocery lists and calenders they would agree to share. Additionally, speech and face recognition will be also allowed by more than 60%. In contrast, most participants of *group 1* would not share their hobbies, login information for social media accounts or websites and their adress or GPS location. *Group 2* is more reluctant. The robot should know as little as possible. The most accepted informations to share are calender entries, grocery list and birthdays. The only information, participants of *group 2* would share more often than *group 1* are login informations.

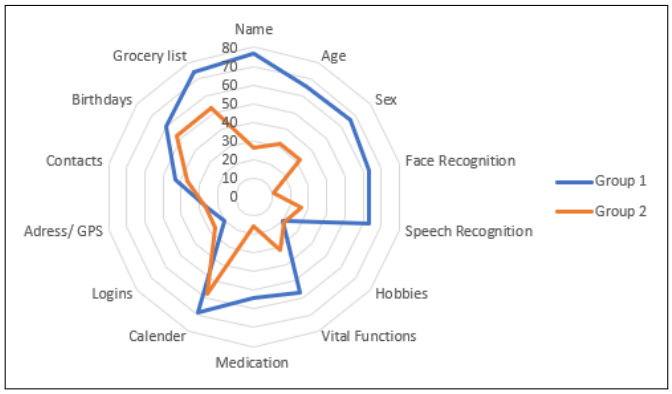

Fig. 5. Personal information, respondents are comfortable with to share with the robot

6.3 Ability of Intervention

In the third section, participants were asked about their interest towards background information of collected personal data. Therefore it will be differentiated between transparency and intervenability. Whereas the transparency questions ask for getting an inside view of collected data, intervenability asks for the ability to modify feature settings and processed information. Transparency is necessary to understand the use and purpose of different features of technical devices. Intervenability allows to exercise the right of informational self-determination by choosing between several data sharing options.

6. I am interested in when the robot is recording.
7. I am interested in what the robot is recording.
8. I am interested in when the robot is storing.
9. I am interested in how the robot uses certain recorded information.

10. I want to decide when the robot is recording.
11. I want to decide what the robot is recording.
12. I want to decide what the robot is storing.
13. I want to be able to turn on / off certain robot functionalities.

6.4 Transparency

Participants would like to have transparency concerning the data robots collect. More than 60% of *group 1* as well as *group 2* agree with most of the statements (see Fig.
reffig:transparency. Whereas the interest in time-dependent personal information for both groups is almost the same, the non-expert *group 2* shows even higher interest in type and intended purpose of personal information. Almost 80% of *group 2* are interested in the data which is collected and they want to know for what reasons and features it is processed and needed. Figure 8 contrasts the

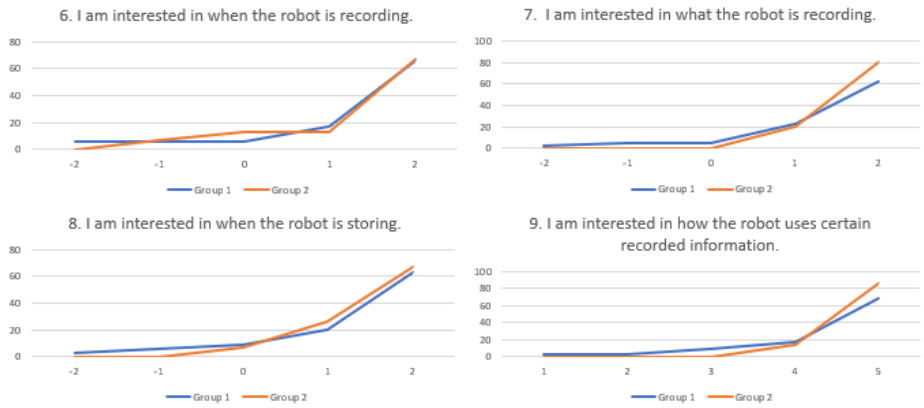

Fig. 6. Transparency for collected and processed personal information

average of both groups. It can be seen, that the average of *group 2* is higher for all of the statements 6 to 9 and the questions *how* and *what* information is used, have the highest level of agreement for transparency.

6.5 Intervenability

The opinions towards intervenability of both groups are slightly different. Again, *group 1* showed a high interest in all possible methods of intervention. *Group 2* is less motivated in this category. They showed a great interest in transparency of personal information, but they do not want to have the ability to entirely control their data. It should be possible to decide when and what personal information is collected, but only 20% care about the storage of this data and for them it is not necessary to turn on/off certain features if they are privacy relevant for example. Again here, only 20% showed an interest for this opportunity. As an interesting factor, Figure 8 shows that the average of question 12 and 13 is higher for *group 2* even though Figure 7 might lead to a different result. This is affected by negative results of *group 1*. Some participants of the robotic group strongly disagree with these statements, whereas no one of the other group did.

6.6 Features and Disclosed Information

In this section the five most requested features and their realization and implementation will be discussed. Therefore three gradations of every feature and the personal information, which needs to be disclosed to make use of it, will be proposed. Figure 9 shows the percentage of users who are willing to disclose their personal information which is necessary for the single stages of the features.

Vacuum Cleaning / Autonomous moving This category will propose two of the features. Because vacuum cleaning requires autonomous movement, these

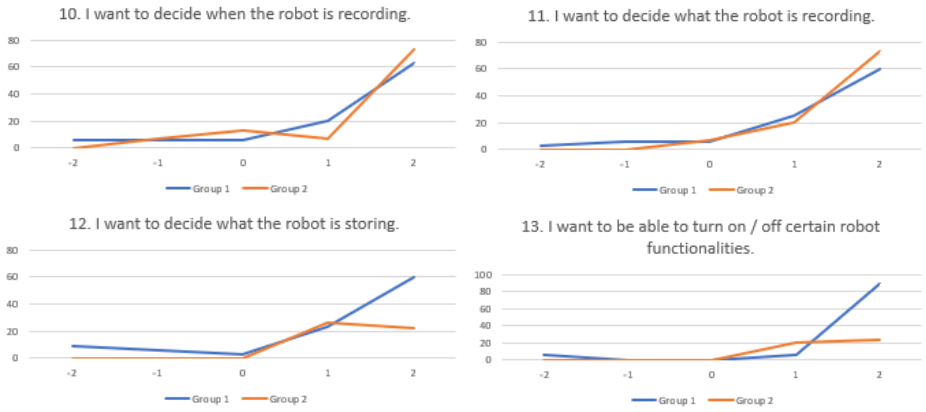

Fig. 7. Intervenability for collected and processed personal information

two features are merged. As already known from Roomba and other vacuum cleaning robots, there are different possibilities of realizing this feature:

1. *Easy cleaning*: The robot drives around in the room or apartment and when it thinks it has finished cleaning, it stops cleaning the floor.
2. *Smart cleaning*: The robot creates a map of the room or apartment and drives through the room in an intelligent way, controlled by an algorithm.
3. *Supervised cleaning*: The robot creates a map, cleans in an intelligent way and additionally, the owner gets information about cleaning status, where the robot already drove and where it did not get.

The general feature of cleaning is requested from 91% of *group 1* and 94% of *group 2*. For the first level of the service no information is needed, but the user cannot check, where the robot has been and where it did not get. For the second level, any kind of sensor is needed, e.g. a laser range scanner or a camera to record home data to create a map. It can also be controlled via Alexa Echo or Google Home. Smart home communication as extra service is allowed by 51% of *group 1* and 21% of *group 2*. If additionally, the robot should be able to transmit personal information to the smartphone, internet and something as a login for the application is needed. Only 12% of *group 1* want the robot to clean the floors, interface with other technologies and would give share their login information. In *group 2*, out of 91%, 5% would use the third level.

Connected Devices In a smart home, devices are able to communicate among one another. Possible levelss in this category are:

1. *Easy communication*: A hub is able to create a local network through which devices can communicate and process their data on a local storage device.

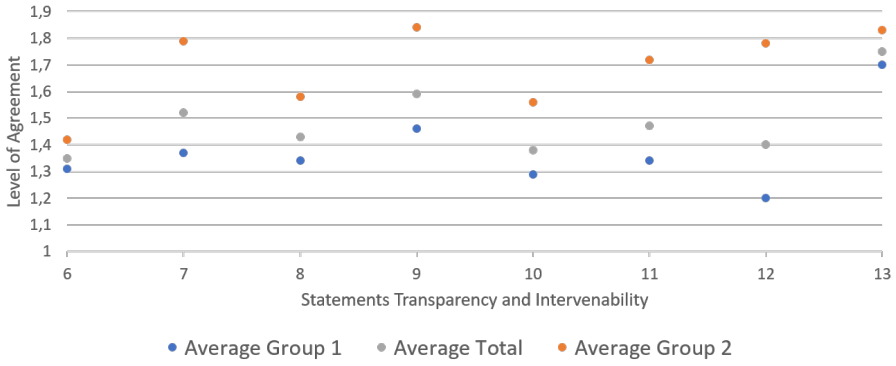

Fig. 8.

2. *Smart communication*: A cloud based approach is able to handle a lot of more and more complex information in a faster way than a local processing solution.
3. *location-based communication*: A location based system is able to track activities of the owner and detects if the owner is near the home, the light or music turns on or the heating or air conditioning is starting.

In a first step, devices are able to communicate inside the home, information is processed on local storage and no personal information is transfered outside the home (74% of *group 1*, 39% of *group 2*). In a second step, being connected to a cloud means being connected to the internet. For using Alexa Echo and Google Home, speech recognition is necessary, which will be sent to a cloud service and analyzed there. This provides a proficient response for all requests in a fast way. Additionally, both services need full access to accounts. 11% of *group 1* and none of *group 2* would be willing to use those devices with this configuration. Thirdly, smart home devices are allowed to track a person, e.g. to adjust the home conditions according to the time of arrival. Excluding full account access, this is allowed by 14% of *group 1*, 0% of *group 2*.

Surveillance in case of emergency Surveillance is a problematic topic. It is categorized in the following steps:

1. *Easy surveillance:* Data can be stored on internal memory and users are able to watch the videostream connecting to the ip address in the same network or it can be viewed later.
2. *Smart surveillance:* Cameras are connected to the internet, process the collected data and give notification in case of detected motions.
3. *Autonomous surveillance:* The system calls for rescue in case of emergency.

The easiest way of surveillance is to be able to take a look at the video stream and see what happens. No special information is needed for that solution. The

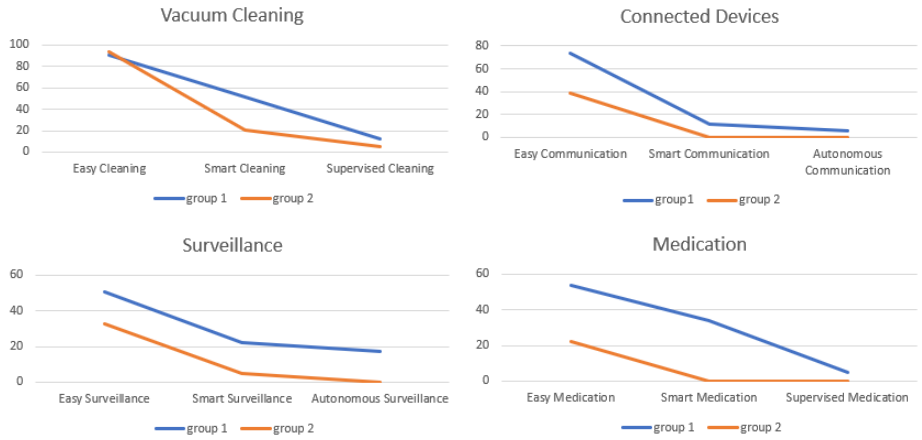

Fig. 9. Gradiations of the features and the percentage of people might using it.

second variant gives the possibility to analyze the video stream and in case of changes or movements it would notify e.g. the user. 22% of *group 1* and 5% of *group 2* would still use this, if devices are connected for communication. In the third stage, an algorithm decides what is shown on the video stream, e.g. emergency or burglary and calls for help. Initially, informed persons can be the user, but also family members, the police or the ambulance might get informed, as already introduced in a similar way with eCall for car crashes. In this case at least emergency numbers needs to be collected. 17% of *group 1* and no one of *group 2* would allow this. (Face recognition is not taken into account in this scenario.)

Medication Next to surveillance, medication is one of the most critical and sensible features. Distinguished can be in this way:

- *Easy medication:* In regular intervals you are reminded to take your medication. This requires, that the user of this application knows which medicine needs to be taken and sets a timer.
- *Smart medication:* If medication needs to be given dependent on the vital status, e.g. blood pressure, personal information needs to be gathered to ensure a right medication.
- *Supervised medication:* One step further is the involvement of an eHealth application where everything according to your health status is stored.

The first feature requires a timer function only. For every medicine a timer with a special name is set, according to intake intervals. 54,3% of *group 1* would use it, only 22,2% of *group 2*. From those who have choosen this feature, all of *group 1* would also allow the information about medication intake, none of *group 2* would. If only the user is allowed to modify these timers, this feature is

uncritical. In a second step, health care status needs to be tracked. Medication often depends on vital functions as blood pressure or blood sugar level. By giving information about medication intake and vital functions, in *group 1* still 34% can use this feature and none of *group 2* would use it, even though 30% of *group 2* would share their vital functions but they did not choose the feature. In a final step, the application is linked to an eHealth application where everything is collected. Therefore it might be necessary to share login information. Only 5,7% of *group 1* would use this feature. Additionally, in case of anomalies, family members or doctors receive a call, when telephone numbers are allowed. Only 5% of *group 1* and noone of *group 2* would allow this.

7 Analysis

Group 1 is more open-minded to use robots. They selected a wider range of features and are more willing to disclose personal information than *group 2*. Participants of *group 1* have potentially the competence to consider that a larger amount of data collection leads to a larger feature set for the robot. Additionally, in case of privacy risks or problems they are able, to intervene on their own.

Group 2 is more cautious. The chosen features are already available, taking a look at Amazon Echo, Google Home, Roomba or other smart home technologies. Although they are using smartphones every day, they cannot assess the risks and therefore only select already known, available features. Interestingly, compared to smartphones, the conservative disclosure of information of *group 2* is surprising. Personal information is shared with applications on the smartphones to gain the full functional possibilities without thinking about privacy risks [9]. Especially in healthcare, people a willing to share their data if that supports a healthy lifestyle [13, 8]. But taking a look at the results of the survey, *group 2* is very reserved. This might lead to the fact, that robots are not in common use for the majority and if they work with robots it is mostly for industrial purposes. Though it needs to be mentioned again, that attitude differs from behavior.

One interesting fact is the distinction between persons. Although 60% of *group 2* wants to have this feature, only 10,5% would allow the robot to use speech recognition and no one would allow face recognition. In *group 1*, 40% of participants would allow both of it.

8 Discussion and Future Work

The questionnaire gave first quantitative hints on user preferences and attitude towards robots. As it can be seen in the results, it almost doesn't matter if people have a technical background. Most of the participants are interested in having a transparent view on the data processed by the robot and they would like to have to possibility to intervene. Even though this survey is not as representative as a user study or a workshop, it shows that users need to be involved during the development process.

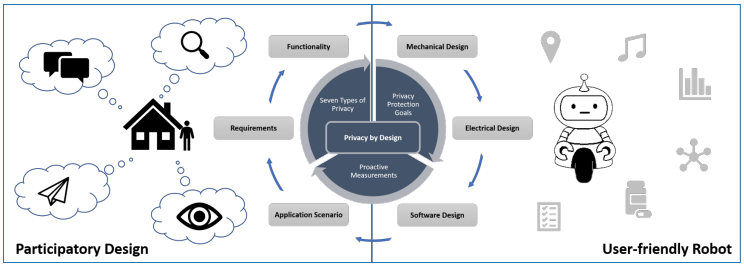

Fig. 10. Development Process

Therefore, as a next step users need to be asked and observed directly. They need to be integrated in the development process to incorporate their perspective. Thereupon, with the help of participatory design strategies, solution ideas need to be developed. As presented, desired features can be implemented on different levels. As one example, distinction between people normally is realized using face or speech recognition. If a user does not want to allow the usage of a camera, there might be less-invasive possibilities to implement the feature, e.g. using RFID tags, specific code words or color identifications. Especially interdisziplinary teams would be able to give new perspectives in robot design and development. Figure 10 shows the overall development process of for privacy protecting robots using a privacy by design apporach.

This allows the user, to get a holistic view of certain features and its capabilities. Users have to be able to be aware of features and its accompanying privacy risks simultaneously. They need to understand and consider actively what happens and how sensors, features and personal information are related to each other. As an example, a red light is blinking when a camera is recording but we only see the content of the video watching it. Installing smartphone applications requires access authorization for camera, microphone and gps sensor - but the purpose of the sensor use is not clearly visible. The questionnaire shows that non-experts does not want to share personal information. On the one hand, this needs to be respected in creating privacy-friendly solutions. On the other hand, sometimes personal information is required but users should be able to decide on its own allowing the access or not. And if the user allows the access, the purpose needs to be clear and the corresponding personal data must be kept confidential.

This survey makes clear, that users should be made aware of common and possible privacy risks because of the imbalance of privacy attitude and sharing behavior [10]. Although both groups are stating their interest about collected data, they do not want to share personal information like location and logins, and *group 2* is critical towards speech and face recognition, there is a gap between attitude and behaviour. As an example, depending on the purpose, users are willing to share their personal data to be able to use different kinds of applications [13, 8, 9]. With the prototype they are able to take a look at certain features and it should be made clear, what sensors are used to provide this fea-

ture and which personal information needs to be collected. With the addition or removal of personal information or processed data, users can get an idea of how the results or operating principles of features change and if they still matche the requirements or if users need to allow more collection of personal data. The more complex a feature gets, the more difficult it is to get a holistic view. An important aspect for introduction of robots is to make people aware of which personal information is needed for specific tasks and how they are protected.

Soon, robots will enter our private homes and going to be part of a smart home. With autonomous movements and decision-making of a robot, it is becoming a very complex and inherant part of our home and our life. Therefore, we first of all need to make people aware of privacy risks and how they can protect themselves. Secondly, there needs to be a possibility to use robots in a privacy-friendly way such that users can decide about functionalities and using a feature on different levels depending on the privacy perception of the user.

Acknowledgment 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)".

References

1. irobot store - roomba980, http://store.irobot.com/default/roomba-vacuuming-robot-vacuum-irobot-roomba-980/R980020.html
2. Alaiad, A., Zhou, L.: The determinants of home healthcare robots adoption: An empirical investigation. International journal of medical informatics 83(11), 825–840 (2014)
3. Alaiad, A., Zhou, L., Koru, G.: An empirical study of home healthcare robots adoption using the utuat model (2013)
4. Aroyo, A.M., Rea, F., Sandini, G., Sciutti, A.: Trust and Social Engineering in Human Robot Interaction: Will a Robot Make You Disclose Sensitive Information, Conform to its Recommendations or Gamble? 3766(c), 1–8 (2018)
5. Bugeja, J., Jacobsson, A., Davidsson, P.: On Privacy and Security Challenges in Smart Connected Homes (2016)
6. Caine, K., Šabanovic, S., Carter, M.: 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. ACM (2012)
7. Caine, K.E., Fisk, A.D., Rogers, W.A.: Benefits and privacy concerns of a home equipped with a visual sensing system: A perspective from older adults. In: Proceedings of the human factors and ergonomics society annual meeting. vol. 50, pp. 180–184. Sage Publications Sage CA: Los Angeles, CA (2006)
8. Chen, J., Bauman, A., Allman-farinelli, M.: A Study to Determine the Most Popular Lifestyle Smartphone Applications and Willingness of the Public to Share Their Personal Data for Health Research 1 22(8), 655–665 (2016)
9. Chin, E., Felt, A.P., Sekar, V., Wagner, D.: Measuring User Confidence in Smartphone Security and Privacy (1)

10. Coopamootoo, K.P., Groß, T.: Why privacy is all but forgotten. Proceedings on Privacy Enhancing Technologies 2017(4), 97–118 (2017)
11. Denning, T., Matuszek, C., Koscher, K., Smith, J.R., Kohno, T.: 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. ACM (2009)
12. Fallmann, S., Psychoula, I., Chen, L., Chen, F., Doyle, J., Triboan, D.: Reality and Perception : Activity monitoring and data collection within a real-world smart home
13. Felt, A.P., Egelman, S., Wagner, D.: I've got 99 problems, but vibration ain't one: a survey of smartphone users' concerns. In: Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices. pp. 33–44. ACM (2012)
14. Geneiatakis, D., Kounelis, I., Neisse, R., Nai-fovino, I., Steri, G., Baldini, G.: Security and Privacy Issues for an IoT based Smart Home pp. 1292–1297 (2017)
15. Heuer, T., Schiering, I., Gerndt, R.: Privacy and socially assistive robots-a meta study. In: IFIP International Summer School on Privacy and Identity Management. pp. 265–281. Springer (2017)
16. Lee, H.R., Tan, H., Šabanović, S.: That robot is not for me: Addressing stereotypes of aging in assistive robot design. In: Robot and Human Interactive Communication (RO-MAN), 2016 25th IEEE International Symposium on. pp. 312–317. IEEE (2016)
17. Lera, F.J.R., Llamas, C.F., Guerrero, Á.M., Olivera, V.M.: Cybersecurity of robotics and autonomous systems: Privacy and safety. In: Robotics-Legal, Ethical and Socioeconomic Impacts. InTech (2017)
18. Lin, H., Bergmann, N.W.: IoT Privacy and Security Challenges for Smart Home Environments (2016)
19. Pino, M., Boulay, M., Jouen, F., Rigaud, A.S.: are we ready for robots that care for us? attitudes and opinions of older adults toward socially assistive robots. Frontiers in aging neuroscience 7, 141 (2015)
20. Smarr, C.A., Prakash, A., Beer, J.M., Mitzner, T.L., Kemp, C.C., Rogers, W.A.: Older adults preferences for and acceptance of robot assistance for everyday living tasks. In: Proceedings of the human factors and ergonomics society annual meeting. vol. 56, pp. 153–157. SAGE Publications Sage CA: Los Angeles, CA (2012)
21. Syrdal, D.S., Walters, M.L., Otero, N., Koay, K.L., Dautenhahn, K.: He knows when you are sleeping-privacy and the personal robot companion. In: Proc. Workshop Human Implications of Human-Robot Interaction, Association for the Advancement of Artificial Intelligence (AAAI07). pp. 28–33 (2007)
22. Theoharidou, M., Tsalis, N., Gritzalis, D.: Smart Home Solutions for Healthcare : Privacy in Ubiquitous Computing Infrastructures (2011)
23. Wu, Y.H., Cristancho-Lacroix, V., Fassert, C., Faucounau, V., de Rotrou, J., Rigaud, A.S.: The attitudes and perceptions of older adults with mild cognitive impairment toward an assistive robot. Journal of Applied Gerontology 35(1), 3–17 (2016)
24. Ziefle, M., Rocker, C., Holzinger, A.: Medical technology in smart homes: exploring the user's perspective on privacy, intimacy and trust. In: Computer Software and Applications Conference Workshops (COMPSACW), 2011 IEEE 35th Annual. pp. 410–415. IEEE (2011)