Transparency for Social Robots

Tanja Heuer[1] and Ina Schiering[1] and Reinhardt Gerndt[1]

***Abstract*— This paper investigates user acceptance and privacy concerns of social robots. Users want a transparent view about processing of personal information. Additionally, they want to be able to intervene. It needs to be possible, to modify default settings. To make users aware of potential risks and concerns it is necessary to involve users during the whole development process and a possible solution for transparency and intervenability may be a privacy dashboard for robots. This privacy enhancing technology provides insight into data processing and sensor use. Additionally, it is necessary to involve users during the development process to sharpen their awareness regarding this issues.**

I. INTRODUCTION

Natural human-machine interaction and social robotics are an emerging field. The first social robots as e.g. the Zenbo[1] already entered the smart home. They are able to control other smart devices at home, tell about the weather, news, appointments, support music streaming and send notifications to family members in case of emergency. To provide this wide range of functionalities, typically robots are employed with a wide range of sensors as cameras and microphones, are using supporting cloud services and connected social media platforms. Hence, social robots collect, process and transfer a huge amount of personal information. Because of the natural interaction with the social robot, which is perceived as a companion by users, this data transfer and processing is not transparent [1]. Also users typically have not the possibility to intervene or do not know how.

According to the Charter of Fundamental Rights of the EU, (Art. 7,8) "everyone has the right to respect for his or her private and family life, home and communications" and "everyone has the right to the protection of personal data concerning him or her". At the moment, these rights of users are not respected by most social robots. The case of Amazon Echo earlier this year gives an example where personal information was sent to someone else without (official) permission [2]. In addition, the General Data Protection Regulation (GDPR) of the EU (2016/679) [3] strengthens these rights in Europe and demand *data protection by design and default*.

In the context of a survey investigating acceptance of social robots and associated privacy concerns, an important aspect are user attitudes towards transparency and intervenability. These two requirements are part of the privacy protection goals [4], which are a common to model privacy requirements. Privacy protection goals are based on the security related goals *confidentiality, integrity, availability* and are augmented by the privacy related goals *transparency, intervenability and unlinkability*. Based on the results of the study, we consider to involve different already existing privacy tools and technologies into the development process of social robots like the privacy protection goals, the seven types of privacy and privacy dashboards to allow transparency.

[1]Ostfalia University of Applied Sciences, Faculty of Computer Science, Wolfenbuettel, Germany, {ta.heuer,i.schiering,r.gerndt}@ostfalia.de

[1]https://zenbo.asus.com/

II. RELATED WORK

A common technology to visualize important information are (privacy) dashboards, which are gladly used by different software applications. This dashboards allow users having an insight view and control about the processing of personal data. They ensure transparency and therefore are an important methodology [5]. An important prototype to investigate usability of privacy dashboards is Data Track [6], visualizing also implications from connected cloud services. With a focus on usability engineering, Raschke et al. [7] presented the idea of a GDPR compliant privacy dashboard. A privacy dashboard for FirefoxOS was proposed by Piekarska et al. [8]. Within a user study, it was investigated how participants make use of the privacy dashboard and what priorities they have. In this context also the Firefox add-on Lightbeam[2], which reveals relations between third party sites on the web is important to note. Additionally, Xu et al. [9] created a smartphone app which summarizes the use of sensors by different applications. The Google Dashboard was investigated [10] with the focus on user acceptance.

Privacy dashboards for smart home applications and smart buildings were developed, to guarantee a user-controlled access [11], [13]. Figure 1(left) shows an example for a smart meter context. In contrast to approaches as data track which try to visualize relations and implications by using a network structure, these privacy dashboards are merely list based. Bier et al. [12] investigate in a user study the interface PrivacyInsight (see Figure1(right)) which is structured similar to smartphone apps compared to a network based and a list based approach. Concepts for ex post transparency including privacy dashboards were furthermore investigated in a broad survey by Murmann et al. [14].

III. METHODOLOGY

In a survey conducted in 2018 during two events, the RoboCup 2018 in Montreal *(group 1)* and in contrast a music festival in Germany *(group 2)*, volunteers were asked about their priorities concerning features, usage and privacy concerns in the context of social robots. A thorough investigation of this survey is beyond the scope of this paper as

[2]https://addons.mozilla.org/en-US/firefox/addon/lightbeam/

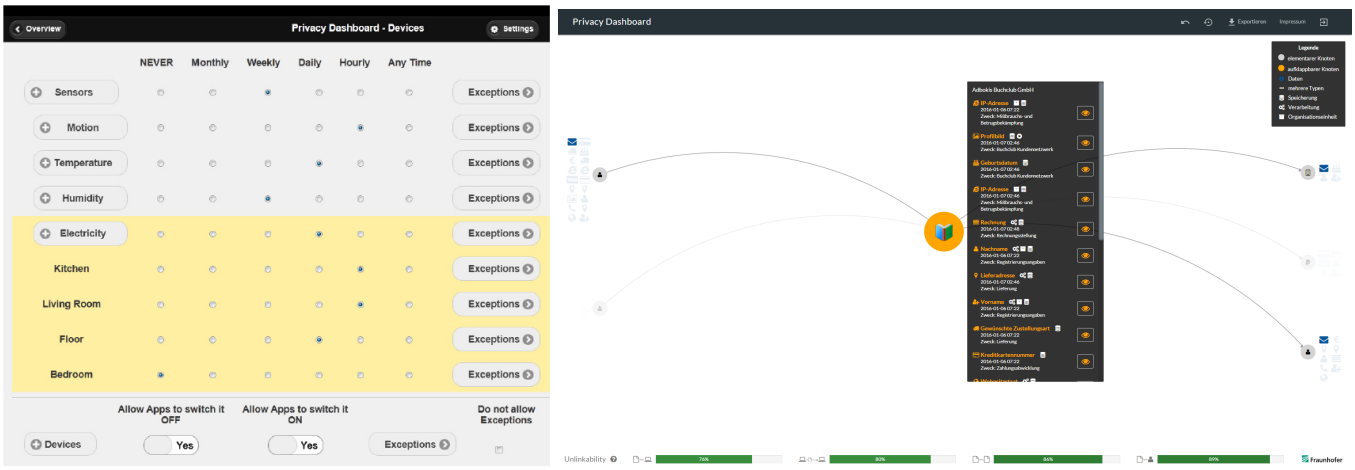

Fig. 1: **(left)** Privacy dashboard of a smart metering system [11], **(right)** PrivacyInsight user interface [12]

ongoing work. The central idea of the two focus groups that were investigated is to query young adults and to compare participants with a strong background in robotics as in *group 1* with a young adults with a standard technical background and no specific experience in robotics as in *group 2*.

The questionnaire used in the study was divided into three sections, the participants were asked about potential functionalities of a robot, interest in using social robots, potential privacy concerns and in the last part demographical information and technical background knowledge. Typically, participants answered the questionnaire in approximately 15 minutes.

In this short paper, the focus is on the investigation of one specific aspect of the survey, namely opinions of potential users towards transparency and intervenability of social robots. Participants were asked to choose their level of disagreement/agreement with the following statements in the range of -2 (strongly disagree) and 2 (strongly agree).

IV. Participants

In total, 73 people participated in the survey, consisting of 35 in *group 1* and 38 in *group 2*. 23 were female, 43 male and 7 decided not to disclose their sex. *Group 1* consists of 7 female, 25 male and 3 non-disclosed participants, *group 2* is divided into 16 female, 18 male and 4 non-disclosed participants. Hence, only 20% of *group 1* is female, whereas almost 40% female participants are in *group 2* . 90% of both groups are aged between 18 and 34.

V. Transparency and Intervenability

Participants of both groups stated that they have substantial privacy concerns in the context of social robots. They expressed a high interest in transparency regarding personal data and the possibility to intervene during the use of robots. As it can be seen in Figure 2 and 3, more than 60% of both groups strongly agreed (rating of +2) with most of the statements. Most of participants of *group 2* do not want to be able to turn on and off certain features of a robot. In comparison, *group 2* showed a general higher agreement on the statements (see Figure 4).

As an unexpected fact, participants of *group 2* showed a higher interest in transparency and intervenability than *group 1*. This effect may have different causes. Whereas *group 1* has a broad experience with robot technologies, *group 2* may be more critical towards the use of robots in their daily life. Robots are not a widespread technology for the general use yet and therefore the attitude towards robots at home is merely skeptical. Nevertheless, the results unambiguously showed, that the participants are aware of the lack of transparency and intervenability and that they want to have access to processed information.

VI. Discussion

In the interpretation of these results, it is important to consider that results of privacy surveys typically differ substantially from actual user behavior. Coopamootoo and Gro [15] investigated in the context of social networks in an empirical study the concepts of privacy and sharing attitude in contrast to the privacy and sharing behavior of users. Additionally, depending on the benefit users feel free to share their personal information [16], [17] and do not think about the risks.

Because of this two facts, it is necessary to involve (potential) users in the whole development process of robots. Because non-technical participants stated, that they are not interested in switch on and off certain features, it is necessary to take them into account. One the one hand, this allows a sensitization of users regarding features, accompanying sensors and it's risks. Users have the ability to shape essential features and the design of the robot. Thereby, they get an insight view into the operating principle of robots. On the other hand, a privacy respecting robot can be developed [18]. To use certain features, special sensors and personal information is needed. Involving the user can lead to a different implementation or to different levels of functionality. As one example, there is a vacuum cleaning robot. Depending on the needs and requirements of the user, there are different types:

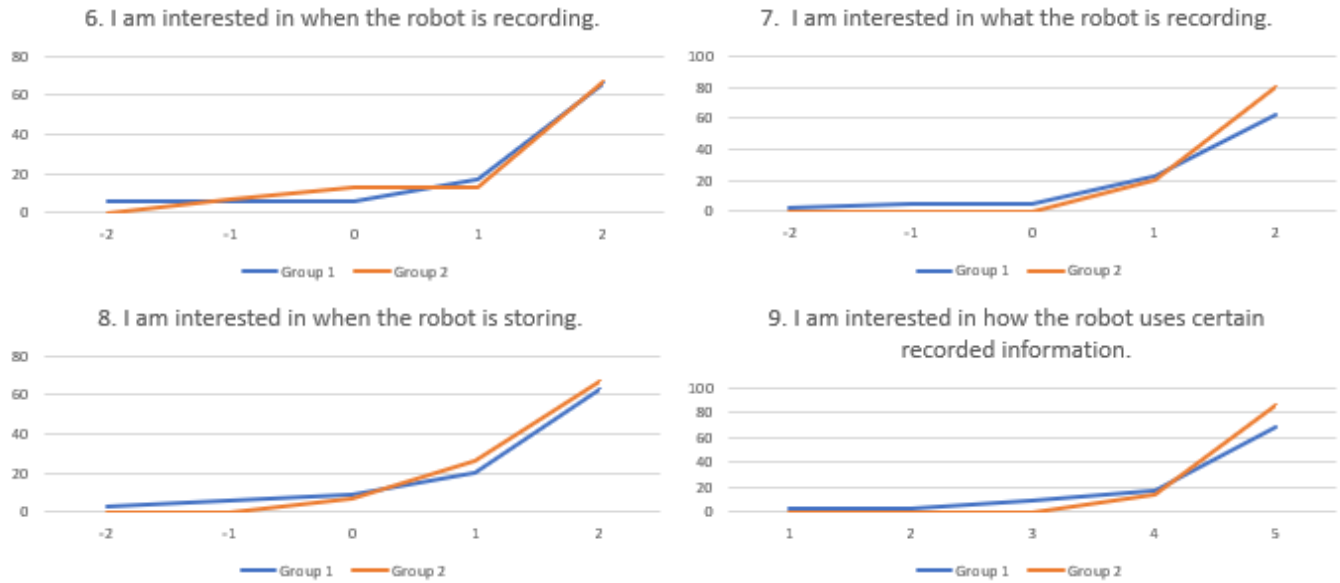

Fig. 2: Transparency for processed personal information

1) *Easy cleaning*: The robot drives around in the room or apartment and when it thinks it is finished, it stops cleaning the floor.
2) *Smart cleaning*: The robot has a laser range scanner and a camera. It creates a map of the room or apartment and drives through the room in an intelligent way, calculated by an algorithm until it has finished.
3) *Supervised cleaning*: The robot creates a map, cleans in an intelligent way. Additionally, the robot can be controlled via other smart home devices and an existing application for the mobile phone informs the owner about cleaning status, where the robot already drove and where it did not get.

Participatory design strategies, which involve the user into the development process, can figure out different needs and gradations regarding the functionalities. Additionally the users see, what is not possible without certain sensors and information and what is. At the moment, most of the existing smart home devices and robots needs to be connected to the internet all the time to allow full functionalities. But it should be possible, to refuse the provision of certain personal information or to disconnect sensors. Instead of complete non-availability, users should be able to decide on their own if they want to have features with only limited and restricted functional capabilities. Robots are able to collect text, videos, images, audio, location, etc. It is important, to get an overview of features and depending data types. Furthermore, it needs to be clear, how the personal data is processed and who has access to it. The purpose of processed data needs to be revealed.

This criteria and it's consequences on the use of the robot can be designed as a privacy dashboard. As shown in Fig. 1(left) for a smart home system, all existing sensors are listed and for every single room/purpose the user can decide on it's own what to allow, when and how often. This needs to be also possible for robots, ideally without a full loss of functionality. Additionally, this should include e.g. restrictions to enter bedrooms, video recording in the bathroom and policies for personal conversations (location-, time-, and situation-dependent). Because users need to be more careful and sensitized about their private life, it is necessary to ask about priorities, preferences and concerns [6], [8], [19]. To allay possible fears of using the dashboard, it needs to be *understandable, easy to use and clearly designed*, that also users without major technical background knowledge are able to use it. They should have co-determination in default privacy settings of the dashboard. This includes predefined privacy settings to protect the users private informations. Because of the complexity of such a dashboard, elements of serious games would be interesting to investigate. This also allows to test the sharing behavior of the user.

All in all, these first conceptual ideas needs to be further investigated. The privacy dashboard for social robots is a step forward to protect life and personal information of the user in their homes in a world full of smart technologies and connected things.

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] M. M. De Graaf, S. B. Allouch, and T. Klamer, "Sharing a life with harvey: Exploring the acceptance of and relationship-building with a social robot," *Computers in human behavior*, vol. 43, pp. 1–14, 2015.
[2] The New York Times, Niraj Chokshi. Is alexa listening? amazon echo sent out recording of couples conversation - may 25, 2018 (visited: 3th september 2018). [Online]. Available: https://www.nytimes.com/2018/05/25/business/amazon-alexa-conversation-shared-echo.html

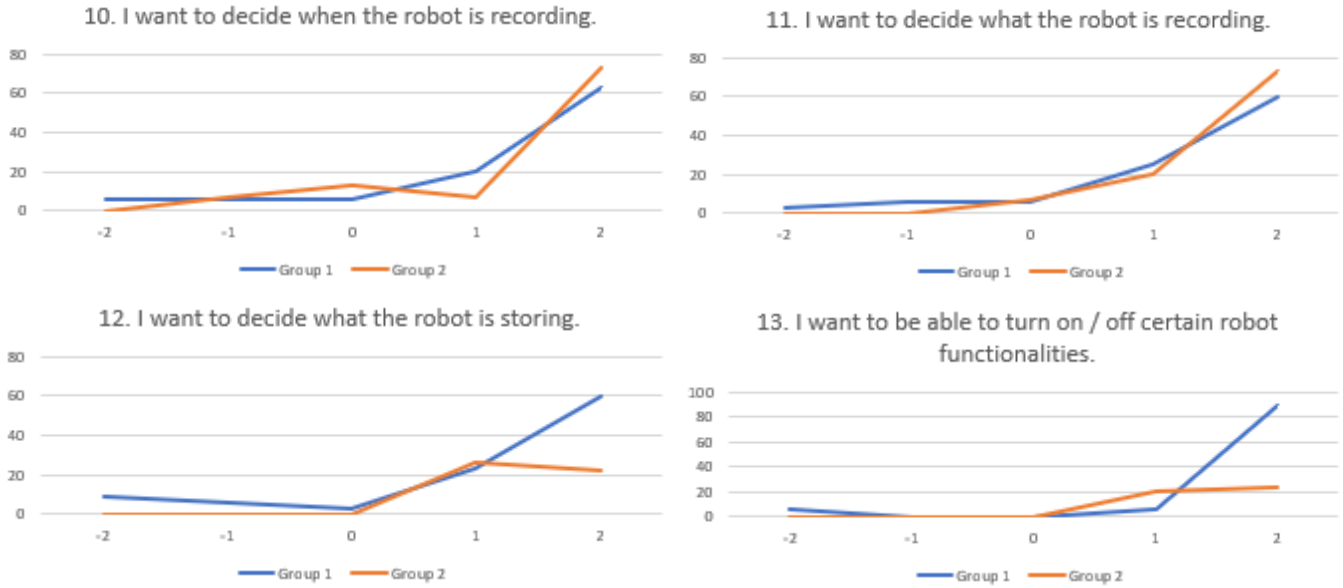

Fig. 3: Intervenability for processed personal information

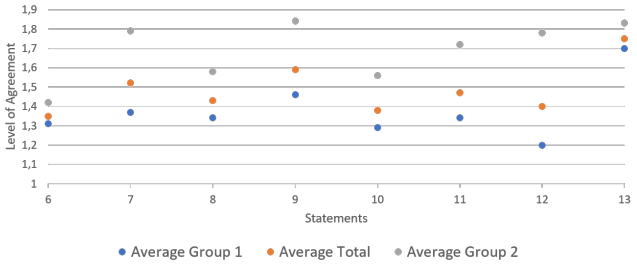

Fig. 4: Average of the Statements

[3] "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.

[4] M. Hansen, M. Jensen, and M. Rost, "Protection goals for privacy engineering," in *Security and Privacy Workshops (SPW), 2015 IEEE*. IEEE, 2015, pp. 159–166.

[5] J. Siljee, "Privacy transparency patterns," *Proceedings of the 20th European Conference on Pattern Languages of Programs - EuroPLoP '15*, pp. 1–11, 2015. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2855321.2855374

[6] J. Angulo, S. Fischer-Hübner, T. Pulls, and E. Wästlund, "Usable transparency with the data track: a tool for visualizing data disclosures," in *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems*. ACM, 2015, pp. 1803–1808.

[7] P. Raschke, K. Axel, O. Drozd, and S. Kirrane, "Designing a GDPR-compliant and Usable Privacy Dashboard," pp. 1–13, 2017.

[8] M. Piekarska, Y. Zhou, D. Strohmeier, and A. Raake, "Because we care: Privacy Dashboard on Firefox OS," *arXiv preprint arXiv:1506.04105*, 2015.

[9] Z. Xu and S. Zhu, "Semadroid: A privacy-aware sensor management framework for smartphones," in *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy*. ACM, 2015, pp. 61–72.

[10] C. Zimmermann, J. Cabinakova, and G. Müller, "An Empirical Analysis of Privacy Dashboard Acceptance: The Google Case," *ECIS 2016 Proceedings*, p. 18, 2016. [Online]. Available: http://aisel.aisnet.org/ecis2016_rp Recommended

[11] P. Ebinger, J. L. H. Ramos, P. Kikiras, M. Lischka, and A. Wiesmaier, "Privacy in smart metering ecosystems," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 7823 LNCS, pp. 120–131, 2013.

[12] C. Bier, K. Kühne, and J. Beyerer, "Privacyinsight: the next generation privacy dashboard," in *Annual Privacy Forum*. Springer, 2016, pp. 135–152.

[13] A. Leonardi, H. Ziekow, M. Strohbach, and P. Kikiras, "Dealing with Data Quality in Smart Home EnvironmentsLessons Learned from a Smart Grid Pilot," *Journal of Sensor and Actuator Networks*, vol. 5, no. 1, p. 5, 2016. [Online]. Available: http://www.mdpi.com/2224-2708/5/1/5

[14] P. Murmann and S. Fischer-Hübner, "Tools for achieving usable ex post transparency: a survey," *IEEE Access*, 2017.

[15] K. P. Coopamootoo and T. Groß, "Why privacy is all but forgotten," *Proceedings on Privacy Enhancing Technologies*, vol. 2017, no. 4, pp. 97–118, 2017.

[16] A. P. Felt, S. Egelman, and D. Wagner, "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*. ACM, 2012, pp. 33–44.

[17] J. Chen, A. Bauman, and M. Allman-farinelli, "A Study to Determine the Most Popular Lifestyle Smartphone Applications and Willingness of the Public to Share Their Personal Data for Health Research 1," vol. 22, no. 8, pp. 655–665, 2016.

[18] T. Heuer, I. Schiering, and R. Gerndt, "Privacy by design for social robots," in *2018 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)(published soon)*. IEEE, 2018.

[19] M. Van Kleek, I. Liccardi, R. Binns, J. Zhao, D. J. Weitzner, and N. Shadbolt, "Better the devil you know: Exposing the data sharing practices of smartphone apps," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 2017, pp. 5208–5220.