Proceedings of the 29th IEEE International Symposium
on Robot and Human Interactive Communication,
August 31 - September 4, 2020 - Virtual Conference

HRI for Legal Validation: On Embodiment and Data Protection*

Yueh-Hsuan Weng, Svetlana Gulyaeva, Jana Winter, Andrei Slavescu, Yasuhisa Hirata

Abstract— **This paper investigates the potential of applying the study of Human-Robot Interaction (HRI) via a "Social System Design" approach to legal issues. A problem when considering AI legislation is that many existing laws were written before the development of AI technologies. To address this issue, we propose examining the effectiveness of laws through the Social System Design approach. Specifically, we will use the General Data Protection Regulation (GDPR) to analyze if any legal gaps emerge when it is applied to social robots. To do so we will employ HRI experiments.**

I. INTRODUCTION

The study of AI law is becoming more and more important as we seek to ensure the safe integration of machines into human life [1]. Due to the limited knowledge of some emerging technologies, as well as influences from legal positivism and legal professionalism, most legal scholars have applied a pragmatic viewpoint when dealing with issues which arise in this area [2]. One side effect of this approach is that it places the focus on revising current laws and neglects the development of new legal codes and norms which may be more suited to dealing with future problems which emerge from increased human – machine interaction [3]. However, there is a gap between current laws and future laws during the transition period for robotics technologies [4]. Naturally it's quite challenging to propose 'future proof' laws. Although some laws can be 'updated' to deal with new technological realities, other developments will require entirely new laws. For example, modern laws for ensuring safety in the use of industrial robots are mainly based on the policy of "human-robot separation". However, in the case of service robots we will need new safety laws that deal with the physical co-existence between humans and robots. One alternative option here is to consider how to introduce the concept of "Safety Intelligence" [5] into our legal framework.

The problem with existing laws is that they lack the ability to validate the effectiveness of legal norms in regard to emerging technologies. Although laws can be changed or revised after they are drafted, law makers often lack the expertise to understand the impact of a given technological development. As a result, they may tend to over regulate emerging technologies.

To examine ways in which we can avoid this outcome we have utilized HRI experiments. The method is called "Social System Design" [6]. One previous study carried out a comparative analysis of the legal impacts of robot experiments in several deregulated urban environments called "Tokku" RT Special Zones [7]. Inside these special zones, law makers can not only simulate the consequences of legal conflicts with robots in advance, but they can also carry out certification for these robots with technical standards in deregulated areas. Through this approach legal accountabilities in regard to autonomous systems can be ensured as well [8].

Apart from the certification with technical standards, norm compliance is the other potential research area for social system design. The International Compliance Association (ICA) defines compliance on two levels. Level 1 is defined as *compliance with the external rules that are impose upon an organization as a whole* and Level 2 *as compliance with internal systems of control that are imposed to achieve compliance with the externally imposed rules* [9]. When we apply compliance rules in combination with privacy laws in the use of social robots, the question of effectiveness arises. When the source of the legal norm is not appropriate to social robots, even if we could successfully realize its norm compliance, it may not be able to ensure privacy protection in HRI. Hence, under the conceptual framework of social system design we propose a sub-concept called "Legal Validation". This allows law makers to quickly validate the effectiveness of current existing laws via a HRI-based legal analytics approach. Legal Validation does not only play a role in trouble shooting, but it also improves the quality control of legislation which relates to the governance of emerging technologies. However, we should be aware the difference between validation and verification. In the field of quality control, validation means: *Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled* and verification means: *Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled*. [10]. In other words, validation ensures "you build the right thing", but not just that "you build it right" [11].

As stated above, we will analyze the General Data Protection Regulation (GDPR) to examine if any legal gap exists in regard to social robots. However, we want to limit the

* This work was mainly supported by JSPS KAKENHI Grant Number 19K13579, and partially supported by the Stanford-Vienna Transatlantic Technology Law Forum, Stanford Law School regarding "Healthcare Robots: A Comparative EU-US Data Protection Analysis". Special thanks to our 32 volunteers from Tohoku University who spent their valuable time in supporting this project.

Yueh-Hsuan Weng is with the Frontier Research Institute for Interdisciplinary Sciences (FRIS), Tohoku University, 980-8579, Sendai, Miyagi, Japan. (e-mail: y.weng@srd.mech.tohoku.ac.jp).

Svetlana Gulyaeva is with Department of Applied Computer Science, TU Dortmund University, 44227, Dortmund, Germany (e-mail: s.gul@mail.ru).
Jana Winter is with Department of Philosophy, University of Vienna, 1010, Vienna, Austria (e-mail: jana.winter@live.at).
Andrei Slavescu is with Department of Psychology, University of Vienna, 1010, Vienna, Austria (e-mail: andrei.sl@gmx.at).
Yasuhisa Hirata is with Department of Robotics, Tohoku University, 980-8579, Sendai, Miyagi, Japan. (e-mail: hirata@srd.mech.tohoku.ac.jp).

978-1-7281-6075-7/20/$31.00 ©2020 IEEE

discussion of legal validation in regard to a controversial legislative issue – embodiment and privacy. When people use consumer electronic products like laptops or mobile phones, their interactions mainly rely on information rendered on a digital display. By contrast, robots use their 'bodies' to provide various visual, audio and physical information points to users. Our main question considers how to use HRI experimental design to validate the effectiveness of existing data protection laws (i.e. GDPR) when these laws have to deal with embodied robotic agents?

II. Related Works

A. Embodiment and Privacy

The embodiment characteristics of social robots allows for new possibilities for human-robot interaction by enabling a wider range of interface development. This impacts their relationship with the law [12] as has been highlighted by Ryan Calo in his paper on robots' emergence in unstructured environments [13]. Additionally, embodiment impacts data governance and privacy in HRI as well. Debora Zanatto et. al. used two humanoid robots – iCub and Scitos G5- to test differences in the trustworthiness of robots to humans. They found that subjects were more likely to interact with robots with a more anthropomorphic appearance [14]. Elsewhere, Pavia et. al. conducted a study that dealt with embodiment and empathy by comparing a virtual agent to a robotic agent. They found that it was more challenging for a robotic agent to perceive the user's emotional state than for a virtual one [15]. In their study Wainer et al. used an empirical approach to investigate embodiment in HRI. They found that people interact with physical robots for a longer time than with virtual animation robots [16]. However, with physical robots at home, users are unconsciously exposing themselves to higher risk environments because their personal information is easily searched and collected. Accordingly, it is crucial we consider the issue of embodiment and privacy in HRI.

Addressing this question, Tonkin's team used two ICT interfaces, a humanoid robot and a tablet, for comparative research. The researchers found that humanoid robots were able to acquire personal information more easily from its users [17]. However, privacy concerns associated with embodiment in HRI are not limited to the appearances of machines and the influences on users. For instance, another issue is that their embodiment might mislead users. Here a laymen's lack of knowledge of a Sanckbot's full frame visual perception with a 360-degree panorama lens [18] is a pertinent example. The acceptance of emerging technology and the factors (age [19], gender, culture [20], health) that affect it can be also an issue [21]. An investigation of embodiment and privacy in human-robot interaction relates to a host of variables. Among them, we chose three variables which relate to privacy in human-robot interaction: deception, proximity, and safety. We present an analysis of these three variables below.

Deception is usually defined as a misleading action. One aspect of deception is the expectation gap that users may encounter when interacting with humanoid or anthropomorphic robots. Embodiment not only plays an important role in building trust but also in improving collaboration between a person and a robotic agent. However, when social robots play the role of healthcare providers or their assistants, they must adhere to the confidentiality and data protection rules. In order to reduce the potential impact on the trust and frustration experienced by people due to the unexpected use of personal information, the functions of the robot that impact privacy should be developed at the design stage and communicated to users in order to make it transparent.

According to the Oxford English Dictionary proximity means nearness in space, time and relationship. For healthcare robots, their algorithmic understanding of suitable proximity to people (based on information from sensors) is crucial in terms of maintaining a satisfactory level of privacy for people interacting with the robot. Therefore, at the design stage in the development of healthcare robots, it is important to consider "privacy spheres" from the point of view of the spatial distance that can exist between robots and humans, so that a person feels that his privacy is not subject to intrusion.

We understand safety as the condition of being protected from danger, risk, or injury. Robotic agents or "Embodied AI" are also safety critical systems. Unwanted system behavior from system integration will lead to consequences in terms of physical security and human injury. The difference between disembodied healthcare AI systems and healthcare robots relates to the integration of software and hardware. Therefore, security by design (software which is developed from the very beginning to ensure safety) is an important factor that healthcare robots should consider during the design and development stage [22].

B. Social System Design

In this Century, robots will gradually enter our living environments until they fully co-exist with humans. Therefore, there is a need to consider how to properly design "robot sociability" [23]. Along this line, a micro viewpoint is to consider such design from bottom-up cases in Human-Robot Interaction [24], such as an accountable system design for AI Transparency [25]. However, in some situations we will need another macro viewpoint of robot sociability by using an "inside-out way". That is to say the subject of design is not robots themselves but rather the many "social systems" in the real-world environments in which these robots are located [6].

C. Data Protection in HRI

The European Union's General Data Protection Regulation (GDPR) is the law that we selected in this case study. A successor to EU Directive 95/46/EC, GDPR was implemented in May 2018. The regulation covers several issues including principles, rights of the data subject (i.e. the right to be forgotten), obligations to data controller and processor, transfers of personal data to third countries and the role of independent supervisory authorities. Among these issues we chose Informed Consent as our testing object for legal validation. Informed Consent, an inseparable part of data protection, is one of the legal bases of the lawfulness of data processing. In Paragraph (a) of Article 6 (1) of the GDPR, it states: *the data subject has given consent to the processing of his or her personal data for one or more specific purposes.* It goes without saying that this is crucial as AI and the IoT play an increasing role in our lives [26].

According to Article 4 (11), the definition of Informed Consent is: *'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*. The constituent elements of a valid informed consent shall match criteria as "freely given", "specific", "informed", and "unambiguous indication of wishes" [27].

This begs the questions if there is any difference when people receive the information on informed consent from a tool like a laptop and a novel product like social robot? We assume that some difference regarding the embodiment might exist between the two technical products, but we don't know yet whether this kind of difference will bring about a legal gap in the governance of data protection and social robots or other embodied intelligent systems. Based on this hypothesis we designed a HRI experiment for the purpose of examining two questions: (1) Does embodiment cause any difference in people's perception of informed consent information? And (2) if there is difference, should we consider a change to current GDPR regulation?

III. METHOD

A laboratory experiment was designed to test our research questions. For the purpose of this experiment, we developed three novel scenarios to test the subjective as well as objective criteria to evaluate the effect of different interaction styles of the robot. Our three scenarios were: "deception", "proximity with bystander", "proximity and safety".

In the deception part, a user is misled by a robot gesture in order to see how the embodiment factor influences the relationship and the HRI when the robot is also an artificially intelligent agent. Another question is the user's attitude to robots as service or assistance providers. In the bystander test, the interaction between the robot and the user is interrupted by a third party, i.e. another user. The aim of this test is to see how different locations and objects (i.e. other people) can affect the HRI and what kind of privacy problems they may cause. As for the proximity and safety test, the user must deal with the engagement zones of the service robot, which are defined in ISO 13482 – a safety standard for personal care robots [28]. The goal of this scenario is to find out how people feel before and after being informed about possible risks, including about greater transparency in the overall system design.

A. Participants

32 volunteers (11 Female, 21 Male) were recruited in Tohoku University. They were aged between 19 and 30 years (M = 23,19, SD = 2.98). The participants had different fields of study. 10 people came from the robotics field. Others came from agriculture, literature, and law. They came from different regions: Asia (China, Japan, Taiwan, Thailand, Indonesia: 15 persons), Europe (8 persons), Middle Eastern (2 Persons) and North and South America (6 persons), Oceania (1 Person).

B. Setup

The study was conducted with a NAO[6] robot by Softbank Robotics using the built-in software. It also utilized a program code for three scenarios using the multi-desktop application *Choregraphe* which created behaviors and monitored and controlled the robot. A Q-Pro Projector was used during one round of the experiment with the goal to show the user the text which was read by the robot. The task was carried out in a room at the Smart Robots Design Laboratory of Tohoku University. Several laptops and one camera were used for controlling the robot and the presentation shown by the projector. The setup with is shown in Figure 1. For laptop testing, an online form called Jotform was used.

Figure 1. Huamnoid Robot NAO[6] and Q-Pro Projector

C. Experimental Procedures

As mentioned, we chose three embodiment variables: deception, proximity, and safety. The experiments aimed to confirm whether these variables cause any legal gaps when informed consent messages are given from a social robot like NAO. There were three rounds of testing with NAO, and another round of testing with a laptop to compare. Note that we randomly choose whether to start from the NAO group or a laptop in order to reduce participants' subjectivity.

Upon arrival, participants were given on overall description of the procedures of the study and were told that they can cancel the experiment whenever they want. They were then given a consent form to read and sign. After giving their consent, they were given an instruction for the first round of testing (either laptop testing or first round with NAO). Afterwards in case there were no questions about the robot or experiment itself they were accompanied to the experiment room. After each round of testing the user was kindly asked to leave the experiment room in order to get further instructions.

Figure 2. The first testing of NAO: Deception

In the first test, *"Deception"*, the user started the experiment with a keyword ("Start" or "Experiment"). The robot's autonomous mode was turned off and it told the participant about the goal of the experiment (receiving a reading of their Chinese zodiac horoscope) and then read the text of the informed consent shown by the projector in front. In order to proceed with the experiment, the user was forced either to give consent or not. If the person agreed to the terms and conditions, the right hand sensor of NAO should be touched. However, the robot raises its left hand, which is on the right of the participant. At this point the user was misled by the robot's gesture. If the participant touched the left-hand sensor, the robot stated "Thank you for your interest and support, the experiment is over now". If the right-hand sensor was touched, NAO read out the participants' 2020 horoscope using the age of the person given during the consent procedure. Before the robot defined the user's zodiac, it tried to guess the participant's age using the face and age recognitions modes. This concluded the first round of testing.

Figure 3.The second testing of NAO: Proximity with a Bystander

In the second round, "Proximity with a Bystander", the user started the experiment with the keyword ("Start" or "Experiment"). Unlike the first round of testing, NAO had its autonomous mode turned on, so during the whole testing he moved slightly more like a human being. The robot told the participant about the goal of the experiment (to become a better version and improve its performance) and then read the text of the informed consent. In order to proceed with the experiment, consent had to be given. In this round of testing the bystander gave consent, though the participant initially is the person the robot is in contact with. Afterwards, NAO took picture of the person who gave the consent. After this part the second round of testing concluded.

In the third round, *"Proximity and Safety"*, the user was asked to choose a comfortable spot for interaction with the robot according to their previous experience in the first two rounds. The spot was marked by a staff member. Unlike the first round of testing, NAO had its autonomous mode turned on, so during the whole testing he moved more like a human being. In this round we considered three engagement zones: first (0-45cm), where it is impossible to give consent, and the robot tells the user that the distance between them is too close and shuts down; in second zone (45-120cm) the robot is talking slowly and the user should speak clearer (voice speed=75, confidence threshold = 48), in the third zone (120cm -) the robot performed as usual (voice speed = 100, confidence threshold = 30).

Figure 4. The third testing of NAO: Proximity and Safety

Depending on which engagement zone the participant chose, the robot either shut down or proceeded with the experiment and then read the text of the informed consent in different voice speeds. In order to proceed with the experiment, consent must be given or not given. When consent is given, we asked the user to take a step back or come closer to the robot, so that in the end the participant has experience in all three engagement zones. Then, the person was asked if there was any difference in the robot's behavior, and where the user felt comfortable considering a difference issue. After this part, the third round of testing with NAO was over.

In the other round of laptop testing that we used for comparing the NAO robot, the participants were required to fill in an online form, where they were supposed to give their consent and to provide their personal data such as name, email address and date of birth. The result (Chinese Zodiac Horoscope 2020) was shown on the laptop screen after consent was given. Also depending on the user's choice, more detailed horoscope including love, career, finance and health predictions could be shown on the screen. After the participants were done with the task, they were asked into a different room to fill in the questionnaire and engage in an informal post-experiment conversation (interview) with one or two researchers.

IV. RESULTS

The data points we collected were (1) Deception: The right or left hand of NAO was touched by the participant; (2) Proximity with a Bystander: The photo NAO took when the consent was given by the bystander; (3) Proximity and Safety: The participants made two choices (X and Y) regarding their 'comfortable distance' in relation to the robot. In addition, we also used questionnaires and interviews to conduct qualitative analysis. Demographic details of the participants such as gender, age, prior exposure to humanoid robots and their personality were assessed using questionnaires. Participants were asked to indicate their level of agreement using a 5-point Likert-scales (1-stronlgy agree, 5 – strongly disagree).

A. Deception

The 32 participants all chose to touch NAO's left hand. With only quantitative data to go on we were not able to address further questions, such as: *Did you touch the left hand because of the of misleading gesture? Why touch the left hand if he/she knew that it was the "wrong" hand?* The scenario had aimed to mislead the participant by raising the robots left hand instead of the right hand in front of the participant. The robot's right hand was mentioned in the visual stimuli ("subtitles") and by the robot's "voice" shortly before the robot lifted his left hand. Also, in the instructions we mentioned that the robot's right hand is indeed his right hand. We also stated that this was to avoid a bias resulting from the general confusion of which is left and which right. Although almost all of the participants noticed the robot lifting his left hand, none of the participants grabbed the right hand.

In the interview we asked why the participants decided to go for the left hand. The participants often could not clearly explain why they grabbed the left hand, although 97% of the participants recognized that this was the wrong hand. The answers were split. Some said it was only intuitive and some said they thought it is a mistake from their side, confusing left and right. Others thought it was a mistake of the study but wanted to go along with the experiment. Others mentioned, that it was impolite to grab the other hand, when the robot was reaching out to them. As we can see, there are multiple answers and the participants themselves were not really sure about their decision either. But this experiment shows that when in question participants would follow the robot's instructions, even though they have heard and read the opposite before. It is worth mentioning here, that this question was not targeted by our study in particular, therefore we can only say that the experiment showed that all people were confused by the gesture and noticed the mistake. It would be an interesting question for further research to investigate.

B. Proximity with a Bystander

Visual stimuli are important factors for robot to understand their physical environment. In the case of privacy protection, the robot's focus person is usually the person it assumes needs to give consent. In this experiment a bystander interfered by giving consent by standing next to a participant. This was to test how the existence of a third party misled robots. Referring to Figure 5, which is a summary of photos of all 32 users, four categories were created: (1) NAO focusing on both parties, (2) NAO focusing on the user only, (3) NAO focusing on the bystander only, (4) The height problem we found in this experiment. Note that "B" means the bystander and "U" means the user.

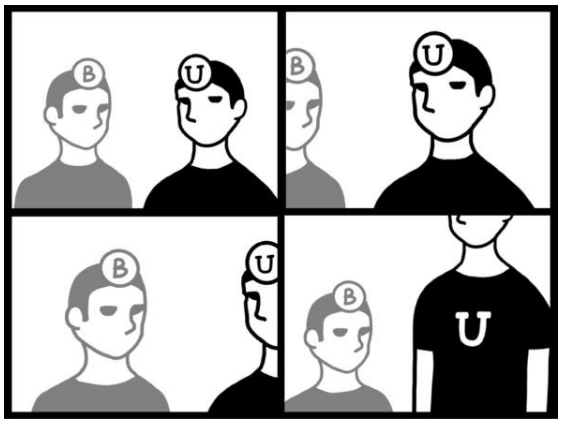

Figure 5. Our results in Proximity with a Bystander

Figure 6 to Figure 8 are details of photos taken by NAO when time consent was given by the bystander. Due to personal privacy concerns, we altered all original photos. In Figure 6, NAO focused on both parties. 13 users fell into this group. Though consent was only given by the bystander, it is a gray zone in informed consent because the two persons exist in the same physical space.

Figure 6. NAO focuses on both parties

Figure 7. NAO focuses on the user only

Figure 8. NAO focuses on the bystander only and The height problem

In Figure 7, 11 users were in the group, NAO only focused on the user. A big privacy concern arose since the robot would lose contact and would register the agreement of the bystander as an agreement to the terms and conditions of the user. In addition, there are two groups in Figure 8. The former refers to the case where NAO only focused on the bystander. Although it appears like an expected result that the consent was given by the bystander, so NAO shall recognize the bystander at the first time. Surprisingly, merely 6 users among 32 persons belong to this group. Finally, to the latter, we noticed another problem that happens when the user is too tall in comparison to the bystander as NAO just skipped his / her face. We called this the height problem.

C. *Proximity and Safety*

This part of the testing aimed to explore a question among potential conflicts between GDPR and ISO 13482 safety requirements of service robots. Therefore, we combined Edward T. Hall's definition of personal distance (i.e. Close phase: 46 cm - 76 cm; Far phase: 76 cm - 122 cm) [29] with the ISO safety measurements in HRI [30]. The actual purpose is to understand people's comfortable proximity zone when a conflict between safety and privacy protection occurs.

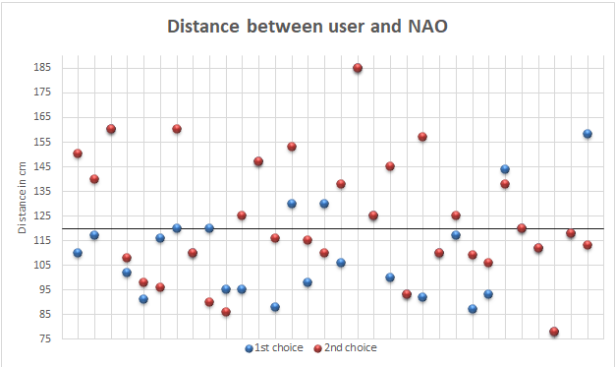

Figure 9. The results in Proximity and Safety

One unwanted situation is that a user wanted to give informed consent to the robot. However, the robot is forced to shut down or reduce its power for user safety when the user stands too close to it. According to interviews, 93% of participants said that they did not feel in danger when they were standing very close to the robot and some even preferred this stance. They were not aware of possible endangerment by the robot. A reason might be that NAO is considered small and cute. Only participants with background in robotics or engineering stated that they want to know more about the robot's functions and that they keep a distance if they don't know the robot yet.

From Figure 9, the only comment that should be noted is that the X axis crosses the Y axis at 120 cm, which is basically the border between the 2nd and 3rd zone. This border line can also act as a reference for legislators to set up where to start safety protective measures in the future.

V. Discussion

There are three issues we would like to discuss here, (1) the influence of the medium; (2) the difference between NAO and a laptop; (3) the results and legal validity of GDPR.

First of all, the applied media were audio-stimuli ("voice" of the robot), visual stimuli ("subtitles" in combination with the "voice" of the robot) and a gesture ("handshake") where the robot moved his arm up in a 90-degree angle to the participant. About two thirds of the participants did not feel distracted by the application of different kinds of media in the study but underlined that they worked complimentarily and were beneficial to their understanding. They did not feel like their attention wandered between the different kinds of media or that they got confused by it.

The participants stated that they would reduce the gesture if they had to reduce one medium and most of them chose audio or the voice of the robot as the most necessary in regard to giving consent. However a lot agreed that the gesture helped enormously to make the process more usable in making it seem more like a human-like conversation. Some even referred to the gesture as a "handshake". Nevertheless, it is necessary to mention that the users had an instruction for what they should do with the arm of the robot beforehand which explained the aim of giving an agreement to the terms and conditions. Only one participant had problems with touching a robot, everyone else was comfortable - often the softness of the sensors of NAO was complimented. Also, only four out of 32 participants were against including a gesture in general, everyone else agreed that it would be beneficial.

It is worth noting here, that participants almost never preferred an audio stimulus if it had not been in English, but their mother tongue. Otherwise, a lot of them went for the visual text format of the projector instead. A lot of the participants noticed that the text complimented the audio stimuli very well; they could check the "subtitles", as some called it, if they did not understand something very well.

Secondly, we asked the participants to compare giving consent with a laptop and with a robot using three adjectives. Afterwards we made two word clouds with this information. The words of our word cloud that described the robot the most in comparison to the laptop were "fun", "interesting" and "easy". But also displayed in big letters were the words "complicated" and "mistakes". The laptop was the mostly described as "easy, boring and normal".

It is noteworthy that there were no negative aspects mentioned except "boring" in the word cloud, and that convenience and quickness were strongly represented. When

the participants had to elaborate a little more, they remarked it as positive that they were more engaged with the robot and had to listen to him more closely. They said that they were paying more attention because the conversation resembled a real human conversation or a lecture. But all of them agreed, that it was boring to listen to the content more than once and that they would like an alteration there.

Figure 9. Wordclouds in two groups: laptop and NAO robot

Some suggested, that the robot(s) at a facility should remember them giving consent and not ask anymore. Also, an option to skip parts or to skim forwards was mentioned. A lot of the participants agreed on skipping the consent if it was an option. Generally, it was marked as a positive to be more aware. A lot of the participants wished to engage more with the robot or to have a more entertaining presentation, but others were concerned that this would harm the serious legal quality of the situation and that people will mistake it for a game.

The autonomous mode of NAO, where he includes gestures and blinking lights to make the conversation more natural, was highly appreciated and agreed upon to make the conversation more natural and fun. Another big aspect of the description of the robot was the "newness" factor. Participants were very excited to use the robot, but admitted that this effect would wear off if one were to engage with a robot on a daily basis. Please note that all of the participants whose answer was indifferent and did not really fit one or the other category were excluded from the total number of the participants regarding each question analysis.

A difficulty in designing HRI for legal validation is that the participants did not understand the problem very well and it took multiple explanations to get across why this is a problem for them. This shows that those kinds of problems are rarely recognized and participants are not aware of this being a legal problem. The answers were split: A lot of the participants said that they would use the robot again, even though they did recognize the problem and would tell their friends and family about it. A significant number of the participants asked for more transparency about the robot's functions, security instructions or function improvement to eradicate the problem before usage. Only few people (3%) said that they feel endangered and that they would not use the robot in a similar scenario again and would also tell their friends and family not to use it. Generally, we can assume that the problem is underrated and not very well understood. Nevertheless, the participants' trust in the robot was affected by this experiment although most participants could not clearly pinpoint the consequences for themselves.

Finally, from our results, it is clear that a robot's embodiment will have an influence on GDPR. First of all, it is necessary to consider social robots or other embodied algorithmic-driven systems as an independent target group in data protection. In the testing of deception, our results show that social robots' embodiment is sometimes problematic for humans. Hence, it creates a new privacy risk. It is something much different to the security risk from information systems or the other existing deception risks by "Social Engineering" [31]. In GDPR's (a) of 5 (1) it states that personal data should be *processed lawfully, fairly, and in a transparent manner in relation to the data subject.* Its Recital 39 also notes that: *The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used.* However, the Informed Consent information provided by NAO covers non-verbal communication, it's beyond the typical scenario of consent given in GDPR, as commented in its Article 7 (2) and Recital 32, mainly based on verbal communication. Hence, the deception issue will cause a legal gap in GDPR when non-verbal communication become more important in consent giving, due to the difficulty in implementing the principle of transparency to data processing. In the case of humanoid robots, to design a plain and easy understandable way of avoiding deception from its Informed Consent processing with humans is challenging. This is because parts of the deceptive consequence caused by human's subjectivity. For example, people with different ages, cultural or educational backgrounds might have different degrees of emotional projection to humanoid robots they interact with.

As for the testing proximity and bystanders, our results show several privacy concerns which may arise. The existence of a bystander or multiple persons in the same physical space with robots or other embodied intelligent systems is another privacy concern. Through our empirical studies we showed that the robot will frequently recognize a wrong person who didn't give consent or will just fall into a gray zone for recognizing both parties. Therefore, it is not going to be a single or rare case. The legal gap is that the data subject has not given his or her consent, but the robot misunderstands that consent has already been given from the data subject. This situation might become general in the near future when service robots provide their service in many public spaces, like hospitals, schools, or shopping malls. GDPR Recital 39 says: *Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing.* Hence, from a data controller's point of view they will have the legal obligation to set up warning notices to data subjects regarding the privacy risk of the bystander effect.

The GDPR also asks if valid consent should be "freely given". In Recital 42 and 43, it states: *Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment* (42); *In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, ...*(43); *Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal*

data processing operations...(43). These clauses mainly focus on ensuring fairness and avoiding monopoly abuse from data controllers [32], but neglects other factors from physical spaces. In our proximity and safety test, one legal gap was that people cannot "freely" choose their comfortable proximity zone to give their consent. Otherwise, robots are forced to shut down or reduce their power when the user stands too close to it. Additionally, the GDPR's harmonization with ISO 13482 might need to be considered as a legislative issue for ensuring future data protection in HRI as well.

VI. CONCLUSION

In this study we designed three different HRI experiments for legal validation. It not only shows a new application of using HRI to improve the compliance of current existing legal regulations, but the potential influence of embodiment on privacy in HRI has also highlighted. However, how to establish a scale to evaluate results in HRI for legal validation purposes must be address in future work.

REFERENCES

[1] Y.H. Weng, C.H. Chen and C.T. Sun (2009) "Toward The Human-Robot Co-Existence Society: On Safety Intelligence for Next Generation Robots". International Journal of Social Robotics, Vol.1, No.4, Page 267-282

[2] Y.H. Weng, T. Izumo (2019) "Natural Law and Its Implication to AI Governance". Delphi, Vol. 2, Issue 3, Page 122-128, Berlin: Lexxion

[3] L. Edwards, B. Schafer and E. Harbinja (2020) "The Future's Already Here, It's Just Unevenly Edited", L. Edwards, B. Schafer and E. Harbinja (Eds.) Future Law: Emerging Technology, Regulation and Ethics, Edinburgh University Press

[4] M. Fenwick, W. Kaal and E. Vermeulen, "Regulation Tomorrow: What Happens when Technology is Faster than the Law?" (2017) 6 American University Business Law Review 3

[5] Y.H. Weng, C.H. Chen and C.T. Sun (2008) "Safety Intelligence and Legal Machine Language: Do we need the Three Laws of Robotics?" Y. Takahashi (Ed.), Service Robot Applications, Vienna: In-Tech, June 2008, ISBN: 978-953-7619-00-8

[6] Y.H. Weng (2018) "Robot Law 1.0: On Social System Design for Artificial Intelligence". W. Barfield, U. Pagallo (Eds.), Research Handbook on the Law of Artificial Intelligence, Edward Elgar Publishing, ISBN: 978-1786439048

[7] Y.H. Weng, Y. Sugahara, K. Hashimoto, A. Takanishi (2015) "Intersection of "Tokku" Special Zone, Robots, and the Law: A Case Study on Legal Impacts to Humanoid Robots". International Journal of Social Robotics, Vol.7, No.5, Page 841-857

[8] U. Pagallo (2017) From Automation to Autonomous Systems: A Legal Phenomenology with Problems of Accountability, Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence (IJCAI-17)

[9] The International Compliance Association (ICA) official definition to "Compliance", available via https://www.int-comp.org/careers/your-career-in-compliance/what-is-compliance/

[10] ISO 9000:2000 Quality management systems — Fundamentals and vocabulary, available via https://www.iso.org/standard/29280.html

[11] CMMI-SVC, Version 1.2, available via https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9067

[12] S. de Conca, E. Fosch Villaronga, R. Pierce, A. de Groot, H. Felzmann, S. Robins, & A. Ponce Del Castillo (2018) Nothing Comes Between My Robot and Me: Privacy and Human-Robot Interaction in Robotised Healthcare. in R. Leenes & R. van Brakel & S. Gutwirth & P.D. Hert (Eds.) Data Protection and Privacy: The Internet of Bodies, Hart Publishing, Page 104.

[13] M.R. Calo (2015) Robotics and the Lessons of Cyberspace, California Law Review, Vol 103. Issue 3.

[14] D. Zanatto, M. Patacchiola, J. Goslin & A. Cangelosi (2016). Priming Anthropomorphism: Can the Credibility of Humanlike Robots be Transferred to Non-humanlike Robots? Proceedings of the 11th ACM/IEEE International Conference on Human-Robot Interaction (HRI), March 7-10, 2016, Christchurch, New Zealand

[15] A. Pavia, I. Leite, H. Boukricha, I. Wachsmuth (2017) Empathy in Virtual Agents and Robots: A Survey, ACM Transactions on Interactive Intelligent Systems (TiiS), Volume 7 Issue 3

[16] J. Wainer, D.J. Feil-Seifer, D.A. Shell, M.J. Mataric (2006) The Role of Physical Embodiment in Human-Robot Interaction. Proceedings of the 15th IEEE International Symposium on Robot and Human Interactive Communication, RO-MAN, pp. 117– 122, September 6-8, 2006, Hatfield, Herthfordshire, UK

[17] M. Tonkin, J. Vitale, S. Ojha, J. Clark, S. Pfeiffer, W. Judge, X. Wang & M.A. Williams (2017) Embodiment, Privacy and Social Robots: May I Remember You? Proceedings of the 9th International Conference on Social Robotics, November 22-24, Tsukuba, Japan

[18] M.K. Lee, K.P. Tang, J. Forlizzi, S. Kiesler (2011) Understanding Users Perception of Privacy in Human- Robot Interaction, Proceedings of the 6th ACM/IEEE International Conference on Human-Robot Interaction (HRI), March 6-9, Lausanne, Switzerland

[19] J.M. Beer, C.A. Smarr, A.D. Fisk, W.A. Rogers (2015) Younger and Older Users′ Recognition of Virtual Agent Facial Expressions, International Journal of Human-Computer Studies, 1; 75: 1–20, Elsevier

[20] Y.H. Weng, Y. Hirata, O. Sakura, Y. Sugahara (2019) "Religious Impact of Taoism on Ethically Aligned Design in HRI". International Journal of Social Robotics, Vol.11, No.5, Page 829-839

[21] W. Wilkowska, M. Ziefle, S. Himmel (2015) Perceptions of Personal Privacy in Smart Home Technologies: Do User Assessments Vary Depending on the Research Method? In T. Tryfonas and I. Askoxylakis (Eds.): HAS 2015, LNCS 9190, pp. 592–603, 2015. Springer

[22] D. Orlando (2018). The Emerging Security by Design Principle in the EU Legal Framework (Master's thesis), University of Oslo

[23] Y.H. Weng, C.H. Chen and C.T. Sun (2007) "The Legal Crisis of Next Generation Robots: On Safety Intelligence". in Proceedings of the 11th International Conference on Artificial Intelligence and Law (ICAIL 2007), Stanford, CA, USA, Page 205-209

[24] Y.H. Weng, Y. Hirata (2018) "Ethically Aligned Design for Assistive Robotics". in Proceedings of the 1st IEEE International Conference on Intelligence and Safety for Robots (IEEE ISR 2018), Shengyang, China, August 24th – 27th

[25] M. Takeda, Y. Hirata, Y.H. Weng, T. Katayama, Y. Mizuta, A. Kojima (2019) "Accountable system Design Architecture for Embodied AI: A Focus on Physical Human Support Robots". Advanced Robotics, Vol. 33, Issue 23, Page 1248-1263

[26] L.A. Bygrave (2017) "Hardwiring Privacy", In Roger Brownsword, Eloise Scotford & Karen Yeung (eds.), *The Oxford Handbook of Law, Regulation and Technology*. Oxford University Press.

[27] H. Miyashita (2018) General Data Protection Regulation, Tokyo: Keiso Shobo

[28] ISO 13482:2014 Robots and robotic devices — Safety requirements for personal care robots, available via https://www.iso.org/standard/53820.html

[29] E.T. Hall (1910). The Hidden Dimension (Vol. 609). Garden City, NY: Doubleday.

[30] C. Harper, G.S. Virk (2010) "Towards the Development of International Safety Standards for Human Robot Interaction, International Journal of Social Robotics, Vol. 2, Issue 3, Page 229-234.

[31] H. Wilcox, M. Bhattacharya (2016) A Framework to Mitigate Social Engineering Through Social Media within the Enterprise, IEEE 11th Conference on Industrial Electronics and Applications (ICIEA), 5-7 June 2016, Hefei, China

[32] L.A. Bygrave (2014) Data Privacy Law: An International Perspective, Oxford University Press.