Privacy First: Designing Responsible and Inclusive Social Robot Applications for in the Wild Studies

Meg Tonkin, Jonathan Vitale, Sarita Herse, Syed Ali Raza
Srinivas Madhisetty, Le Kang, The Duc Vu, Benjamin Johnston, and Mary-Anne Williams

Abstract— **Deploying social robots applications in public spaces for conducting in the wild studies is a significant challenge but critical to the advancement of social robotics. Real world environments are complex, dynamic, and uncertain. Human-Robot interactions can be unstructured and unanticipated. In addition, when the robot is intended to be a shared public resource, management issues such as user access and user privacy arise, leading to design choices that can impact on users' trust and the adoption of the designed system. In this paper we propose a user registration and login system for a social robot and report on people's preferences when registering their personal details with the robot to access services. This study is the first iteration of a larger body of work investigating potential use cases for the Pepper social robot at a government managed centre for startups and innovation. We prototyped and deployed a system for user registration with the robot, which gives users control over registering and accessing services with either face recognition technology or a QR code. The QR code played a critical role in increasing the number of users adopting the technology. We discuss the need to develop social robot applications that responsibly adhere to privacy principles, are inclusive, and cater for a broad spectrum of people.**

This research is supported by an Australian Government Research Training Program Scholarship, an ARC Discovery Grant and a UTS BlueSky grant. We thank Jobs for NSW, the Sydney Startup Hub team and the participants for giving us the opportunity to conduct this study.

The authors are affiliated with the Faculty of Engineering and IT of the University of Technology Sydney at the Innovation and Enterprise Research Lab - Centre for Artificial Intelligence (e-mail: margaret.tonkin@student.uts.edu.au).

I. INTRODUCTION

In the wild studies with social robots are increasing in number and variety: studies have been undertaken in airports [1], [2], shopping centres [3], [4], public services [5] and hotels [6], to highlight just a few. Designing purposeful, real world social robot applications for these studies is a difficult undertaking. However, it is of considerable importance to ensure meaningful outcomes for research, industry, business and society [7].

Creating real world social robot applications for public spaces requires careful study and understanding of the environment in which the robot is to be deployed to ensure a viable application and a positive customer experience for the situational context [2]. Social robots can create experiences unique from other technologies through a combination of communicating in a socially natural, human fashion [8] and all the psychological aspects this type of interaction includes, while also digitally communicating and providing an interface to technological devices around them. The challenge is to create an application able to ensure the best customer service and experience in the considered environment, that utilises both social and digital communication in an appropriate fashion.

In this study we explore potential applications in a government managed centre for innovation and startups. We approached the development of social robot applications with a human centred design focus [9] and followed the user experience design (UX) methodology for human robot interaction [2] to uncover unmet user needs and insights. These were used to determine viable social robot applications to enhance the user experience for entrepreneurs and visitors within the centre. We discovered that before we could provide any type of real world application for use in the location, we needed to address the issue of privacy management because our applications would require permission of users to store their personal information.

Thus, in this paper we present our findings from the first iteration of our prototype, namely the user registration and login system. In fact, without such a system a social robot interacting with multiple users visiting the considered public space would not be able to provide personalised services to users or be sociable. Importantly, given the nature of the robot's utility in the public environment, the system must be inclusive, i.e. guarantee fair access to its services within that environment, and comply with local privacy laws. Hence our research question is: "How might we design a registration and login process that responsibly collects necessary private information while adhering to privacy regulations and providing inclusive services"?

In the following section, we address our research question with a discussion on the challenges of privacy, the importance of transparency and the impact of trust for robots deployed as shared resources in a human-centred public environment.

II. Robots as shared resources: Privacy, transparency and trust

As robotic technology and platforms continue to develop in complexity, function and scale, it is vital that responsible methods for data collection that protect privacy and preserve fairness, are developed [10], [11], [12]. Article 12 in the United Nation's Universal Declaration of Human Rights (UDHR) details the Right to Privacy of all people [13]. Respecting the human right to privacy is a significant challenge for roboticists as robots are effectively powerful surveillance devices [14] able to collect visual, audio and situational data, for analysing and responding to their environment. Studying privacy in Human-Robot interactions is an emerging area of research, recently referred to as ”privacy-sensitive robotics” [15], [16].

When a robot is installed as a shared resource in a public space and provides people access to personalised services, the subsequent collection of customer data brings consumer privacy issues to the fore. This is particularly the case for the collection of sensitive biometric information, such as facial information required for face recognition technologies. Collecting face data requires explicit consent from the user under European regulations, with increased regulation of consumer biometric data expected from other countries [17].

To meet required privacy regulation, users need to be aware of how personal information collected will be used, retained and shared (by the organisation behind the technology), and to understanding the privacy implications of using the system [12]. Transparency assists users' risk assessment and their decision of whether to trust, and consequently adopt, the designed robot application. In addition, transparency has been demonstrated to positively impact on users' experience [12].

Previous research has outlined transparency as a tool to promote user trust of new systems and the companies making them; with this being particularly true for systems collecting private user information [18]. It has been suggested that in this context, a strengthening of consumer trust towards an organisation grows from the quality disclosures that result from transparent protocols [19], [20]. This may enhance the perceived trustworthiness of the organisation to users, so long as the company abides by their own outlined practices [21].

The impact of consumer trust on the adoption of new technologies is a genuine and growing concern within social robotics. If users do not trust a new system, its acceptance and integration into the public may be met with resistance [22]. When collecting personal information, trust affects the users willingness to risk disclosing private information to a system [18]. It is imperative that the organisations behind these technologies strive to build strong, long-term relationships with users; allowing them to feel comfortable enough to rely on these institutions to protect their interests and information [19], [23].

Issues surrounding trust towards new technologies may occur due to various factors. Most notably, the perceived competency of a new or newly emerging technology can have great impact on user trust [24]. The current social climate surrounding autonomous cars is a clear, real-world example [25]. Additionally, the trust (or distrust) felt by a consumer towards a company can have flow on effects towards the products that the company designs and develops [18].

Developing a responsible social robot application for personalised use in a shared environment requires strong consideration of possible privacy impacts. The transparency practices used should also be examined for their impact on user's trust and subsequent adoption of the new system.

III. Registration System Design

User registration systems for login processes are nothing new. People register personal details with websites, mobile apps and company software everyday, and the practice is quite established. However, registering as a user for a robotic application that uses facial recognition is an undertaking that is not common and it introduces additional challenges in privacy.

In the wild studies for robots that use registration systems for personalised services are not new but few in number. Glas et al. undertook a study in a shopping mall that used a mobile application to register users, enabling them to request the services of a baggage carrying robot [26]. However, users were hired for the study, instructed what tasks to perform and were not general customers of the shopping mall. Hybrid-cloud systems that combine robotics platforms, web portals and mobile apps, such as that by Fiorini et al. [27], are more recent yet still limited in number, although of great interest in the aged care and medical health domain.

Our main differentiation from the aforementioned works is to offer our users different methods to access the system to guarantee maximum inclusiveness, and a way for users to manage their information, that complies with locals laws and privacy regulations regarding sensitive data.

To determine the right design for our registration system we look to Nissenbaum's theory of ”contextual integrity” suggesting that privacy expectations are mainly determined by social norms of information flow for specific contexts [28]. Therefore we concentrate our user registration system design on the idea that privacy expectations are context-specific, and that the information to be collected must be germane to the particular purpose of use and specific community, based on social norms for the information flow that may be expected in the environment. However, as social robots are a new experience for most people, social norms for the information flow between users and a social robot have not yet been established. Hence, we assume that there will be a certain distribution of the population [29] that will be reluctant to use their face as their personal identity due to their risk assessment of the unfamiliar situational context, with a possible lack of trust in the management of their information. So we identify an alternative methodology to provide access to the services that reduces the amount of sensitive information required from the user. We offered users that did not want to register with their face to use a QR code instead. Users that selected the latter option were not automatically recognised by the robot. Instead they gained access by showing a QR code from their smartphones to the robot. The QR code alternative impacts the user experience, as the login system is less immediate and less social (between robot and user), but still guarantees access to the provided services, thus enabling maximum inclusiveness among all users.

Performing an evaluation of possible privacy impacts and risks, as per a privacy-by-design approach [30], and recommended for robot user experience design (UX) [2] allowed us to identify how personal information would flow in the proposed robot application and identify options for maintaining contextual integrity, minimising negative privacy and UX impacts. This included determining which type of information should be provided (name, face information, e-mail, mobile), when (which step of the process), and where is appropriate to do so (on the robot on-site, or elsewhere on a different device, e.g. mobile or laptop). Additionally, considerations such as security and minimising identity misuse by bad actors meant creating a two-step registration process. Hence our robot registration system is diversely cross-platform: combining robotic, mobile and web platforms.

We measured the success of the proposed system by counting the number of people that completed the registration process on the robot by choosing either to register with their face or with a QR code, as opposed to leaving the registration process due to a lack of desirable alternatives. We also measured the sentiments and feelings of individuals that registered to monitor the functionalities to maintain, abandon and/or pivot, as per the design methodology by Tonkin et al. [2].

Our contribution in this paper is the provision and discussion of a viable design for a cross-platform registration and login process for social robot applications able to 1) maximise the inclusiveness of the system among the targeted audience; 2) meet privacy regulations regarding the collection, storage and use of sensitive information; and 3) elicit positive sentiment from users regarding the registration process experience. We deployed this registration system for use in the wild and our study design is described in the following section.

IV. Study Design

We situated our study at the Sydney Startup Hub (SSH), a government managed centre for startups and innovation. We employed a humanoid Pepper robot to register the identities of SSH's visitors that wanted to use the robot. The robot was placed next to the reception desk where it was visible by people entering the reception area. Behind the robot was a vertical coloured banner alerting people to the presence of a social robot research study endorsed by logo of the university sponsoring the study (Figure 1). The researchers monitored the robot from a seating area next to the reception desk. The robot offered users two options to register their identity: 1) by capturing their facial information, or 2) by sending a QR code to show to the robot as login. We conducted the study by exhibiting the robot at the location during business hours (i.e. Monday to Friday from 10am to 5pm) for a total of seven business days.

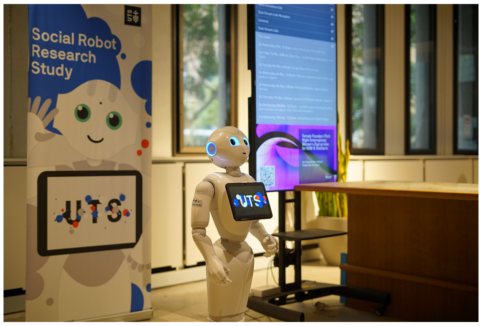


Fig. 1: The location of the robot during our study.

A. *Participants*

SSH visitors were free to approach the robot, which was programmed to greet and engage with the users detected at approximately 1.2 meters from the robot camera. When a user was detected and greeted by the robot, the user was invited to take part in the study. If not interested, users were free to leave.

If the participant remained engaged with the robot to continue the interaction, the researchers approached the participant to provide them more information about the research study and a participant information sheet, as per protocol approved by the Ethics Committee of the University of Technology Sydney. The participants then interacted with the robot without receiving instructions by the researchers. The robot was completely autonomous. Before proceeding with the registration process, the robot asked the participants to read a digital consent form and to press a button to either agree or not to continue with the research study. To accept the consent form the participants had to be over 18 years old and able to communicate in English. After giving informed consent, the interaction continued with the registration process as described in Section V-A, below. Participants registering on the robot were asked to verify their identity and complete their registration on-line.

Participants were able to start the registration process from the on-line website, and then complete it by visiting the robot on-site. In this case, the informed consent was presented during the on-line registration process. Hence, in this study we included all the participants' that accepted the digital consent form on either the robot or the on-line website and they:

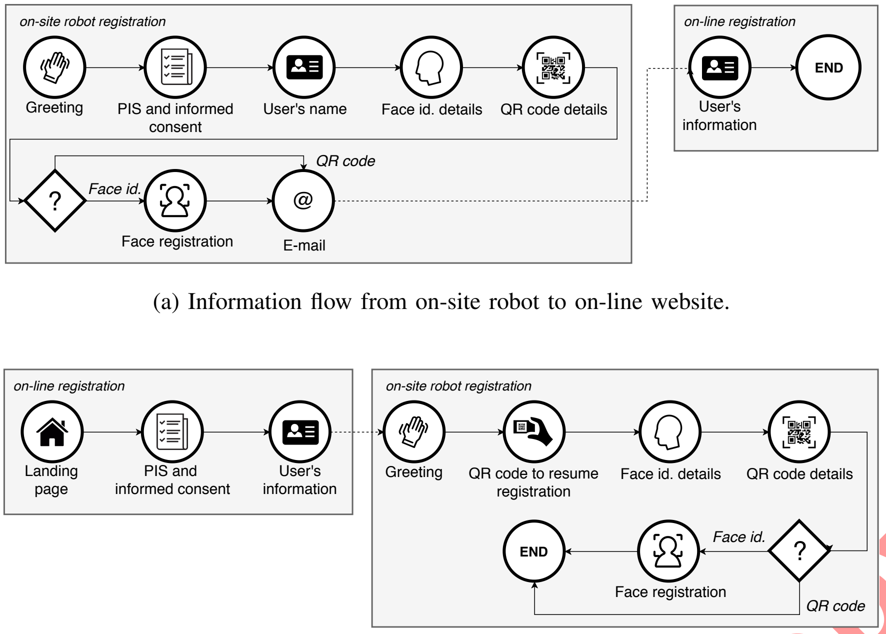
1) fully completed the registration process on the robot; *OR*
2) fully completed the registration process on the on-line website; *OR*
3) initiated the registration process on the robot but left after receiving information about the face registration option.

The third condition was necessary to measure how many participants left the registration process after receiving details about the use of face recognition, which is considered sensitive data collection. A total of 103 participants interacted with the robot and an additional 3 participants registered on-line; thus, a total of 106 participants were included in the study. For this study, we did not collect the gender and age group of our participants.

B. *Measures*

To investigate users' registration preferences, we measured the number of people who decided to register with their face, to use the QR code, and to leave the registration process when becoming aware of the offered options for completing their registration. A measure of success for our design would be to maximise the number of users that completed the registration process by choosing one of the two available alternatives.

To better understand the users' choices and evaluate the user experience of the registration process, we collected qualitative feedback from the registered users through a post-interaction survey. The survey included



(a) Information flow from on-site robot to on-line website.

(b) Information flow from on-line website to on-site robot.

Fig. 2: Designed registration information flows

the following items:

- a 5-point Likert scale ranging from “very particular” to “very open” measuring how participants described themselves with regards to sharing their private information;
- an open-ended question asking to provide feedback regarding the experience of registering with the robot;
- an open-ended question asking to describe why the user selected face identification or QR code.

C. On-line Pilot Study

We ran an on-line pilot study on Amazon Mechanical Turk to test if the designed alternatives to register with the robot were suitable for the considered study.

We recorded a video of a Pepper robot enacting part of the registration process employed in this study. In the on-line pilot study we introduced the robot as a device situated in the participant’s work environment allowing the access to personalised services for the workspace. On-line participants and the study participants obtained the same details about the two registration alternatives.

We asked the on-line pilot study participant to select to register with either face identification or QR code and to motivate their choice with an open-ended question. We were particularly interested to discover the presence of ceiling or floor effects among the two alternatives and users’ motivations for their choices.

From the total 274 participants about 74% selected to register with face identification and the remaining 26% with QR code. No ceiling or floor effects for either of the options were found. The most recurrent motivation among people choosing face identification was its ease of use and time convenience, whereas participants choosing QR code suggested that this option was less privacy intrusive and more reliable in dealing with look-alike individuals.

V. Registration Process

The registration process required two steps: 1) registering a password and entering some personal information on an on-line website deployed specifically for this study; 2) registering the access preference to the system (i.e. face identification or QR code) by physically interacting with the robot on-site. People were free to choose the order and when to perform such steps. However, users were not able to access the services offered by the robot until they completed both required steps. Figures 2a and 2b summarise the two possible interaction flows for the full registration process.

A. On-site Robot Registration

When the robot detected the face of a person at approximately 1.2 meters, it greeted the users while briefing them about the research study. Meanwhile, the face recognition system analysed and compared the face of the current user with previously registered faces. If the system found a match with a face in the robot's database, the robot paused then acknowledged the user by name. If the recognised user had also completed the on-line step, the robot allowed the user to access a menu with a list of provided services. Otherwise, the user was reminded to complete the on-line registration before being granted access to the services.

If the face recognition system did not match the user's face with any of the registered faces, the robot offered the user the option to continue with a QR code or to register as a new user. Users received a valid QR code to use when completing the on-line registration process. The QR code was used in three scenarios: 1) by users registered only on-line to resume and complete their registration process on the robot; 2) by users selecting QR code as their access method and completing the registration on-line; 3) by users selecting face identification as access method and completing the registration on-line, but unrecognised by the robot. This latter option was used as a fallback for managing false rejections by the face recognition system.

New users selecting to register on the robot were first asked to provide their name, so the robot correctly addressed them during the rest of the process. This step was neglected for users that already completed the on-line registration.

The robot then provided information on how the face recognition system works and the employed privacy policies. This step was crucial for adhering to current privacy legislation and to enhance the user experience, as evidenced from our previous studies [11], [12]. Following this, the robot provided details on how QR code access worked.

After presenting the two available alternatives to complete the registration, the robot asked the participant to select their preferred access method. If the user selected face identification, the robot asked them to stand still and look into the forehead camera to register their face. If the user selected QR code this step was skipped.

To complete the registration process, the user needed to provide a valid e-mail address to receive a link to complete the registration on-line. This step was skipped for users that already completed the on-line registration.

Importantly, all registered faces were stored locally on the robot and never transmitted on the internet. Also, the system removed all other information collected from users at the end of the registration process.

B. On-line Registration

The on-line registration website opened with a landing page showing a button to login for registered users and a button to register as a new user. The landing page also offered information about the Pepper robot, the research study, the research team and the research partners.

Users selecting to register were asked to read a participant information sheet and to provide consent before proceeding. This step was not required by users that already completed registration on the robot, since they were already asked to do so while registering on-site.

Users were then asked to provide an e-mail address, a password, their name (pre-filled if already supplied during the registration process from the robot on-site) and, optionally, a mobile number and the name of their business.

Users completing the registration on-line were able to edit or remove their profile at any time. They were also able to retrieve a QR code to complete the registration on the robot (and to use it to access the robot services, if they decided not to use face identification). Through the website, users were also able to answer our post-interaction survey. In addition, the website provided access to our privacy policy.

VI. Results

We counted the number of participants interacting with the robot, accepting the consent form and either completing the registration on the robot or abandoning it after getting to know details about the face identification process. Table I reports the number of participants interacting with the robot and included to our study, together with their preference for registering with the robot.

TABLE I: Participants and their access method preference.

	Face identification	QR code	Left	Total
N. participants	78	18	7	103
% participants	75.73%	17.47%	6.80%	100%

Among the participants completing the registration on the robot 78 out of 96 (81.25%) selected face identification. We tested if this choice was above chance level by employing a single sample z-test for proportions. The selection of face identification against QR code was significantly above chance ($p < 0.01$).

Due to our two-steps registration process, our participants fall into two main groups: 1) those initiating the two-steps registration process from the on-line website, and 2) those initiating the two-steps registration process directly on the robot. Therefore, we collected the number of participants that either completed both the required steps or only one of the two required steps (i.e. only the on-line registration or only the robot registration). Tables II and III show the amount of participants initiating the registration process from the on-line website, and the amount of participants initiating the process on the robot, respectively.

TABLE II: Participants starting from the on-line registration.

	Two-steps completed	Two-steps not completed
N. participants	0	3
% participants	0%	100%

TABLE III: Participants starting from the robot registration.

	Two-steps completed		
	Face identification	**QR code**	**Subtotal**
N. participants	44	11	55
% participants	45.83%	11.46%	57.29%
	Two-steps not completed		
	Face identification	**QR code**	**Subtotal**
N. participants	34	7	41
% participants	35.42%	7.29%	42.71%

We tested if the chosen registration flow (web first

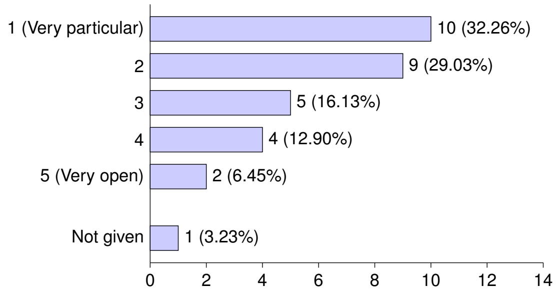


Fig. 3: Self-report of participants' private information disclosure level.

vs robot first) and the outcome of the registration (completed vs not completed) offered any dependency. Given the small sample size of users initiating their registration process from the website, we conducted a Fisher's exact test which suggested that the relation between these variables was not significant ($p = 0.0844$).

A chi-square test of independence was performed to examine the relation between the chosen access methodology (face identification vs QR code) and the registration outcome (completed vs not completed) within the group of participants initiating the registration process on the robot. The relation between these variables was not significant, $\chi^2(1, N = 96) = 0.1321$, $p = 0.7163$.

Among the 55 participants completing the two-step registration process, only 31 of them (56.36%) completed the post-interaction on-line survey. Furthermore, among the participants completing the on-line survey, 28 participants were those that selected face identification, whereas only 3 were those that selected QR code access.

The post-interaction survey asked participants to rate themselves on how open they are to share their private information on a scale from 1 ("very particular") to 5 ("very open"). Figure 3 shows the distribution of their answers.

We also asked participants completing the on-line survey to provide feedback about their robot interaction experience. When analysing the provided feedback we extracted the adjectives used to describe the experience and categorised them into positive adjectives or negative ones. Some of the comments included multiple adjectives. Table IV shows the adjectives describing the experience with the robot.

TABLE IV: Adjectives counts as provided by participants to describe their interaction with the robot.

Positive adjectives						
Fun	**Great**	**Easy**	**Straightforward**	**Fast**	**Engaging**	**Novel**
4	3	2	2	1	1	1
Unique	**Surprising**	**Sociable**	**Reasonable**	**User-friendly**	**Simple**	
1	1	1	1	1	1	

Negative adjectives					
Slow	**Talkative**	**Unresponsive**	**Long**	**Instructional**	**Limited**
6	1	1	1	1	1

Participants described their experience with the robot by using a total of 19 adjectives: 13 denoting a positive experience and 6 denoting a negative one. In total, the adjectives were used 31 times in the participants' comments, with a count of 20 denoting a positive experience (64.52%) and 11 denoting a negative one (35.48%). Three participants also expressed discomfort when interacting with the robot due to the short height of the robot and their need to bend when typing their name or the e-mail address. Furthermore, four participants provided an adjective to describe the robot in their feedback. Pepper was described as charming, cute, adorable/friendly, and intimidating.

Finally, we asked the participants completing the on-line survey to justify why they selected face identification or QR code during their registration. By reading the provided motivations we identified seven main reasons: 1) convenience/accessibility; 2) novelty; 3) curiosity; 4) social nature of the interaction; 5) fun; 6) trust; and

7) security. Some of the provided comments reported multiple explanations, that fell into more than one identified category. The results of this qualitative analysis are shown in Table V.

TABLE V: Participants' motivations for choosing face identification or QR code.

	Face identification	QR code
Convenience/accessibility	20	1
Novelty	4	0
Curiosity	3	0
Social nature of the interaction	2	0
Fun	1	0
Trust	1	2
Security	1	0

Interestingly, two of the three participants that selected QR code justified their choice by suggesting that they did not have sufficient trust to register their face. We report their answers here for convenience:

> *"I choose QR code because I don't trust face recognition system if they can get hacked easily"*;
>
> *"I won't give my Face ID to a service provider I can't fully trust"*.

VII. Discussion

Our results clearly show people's preference for face identification when registering with our system. In fact, 78 out of 96 participants (81.25%) who completed the registration process on the robot choose to register their face information instead of using a QR code. This choice was well above chance. Nevertheless, although face identification was the most privacy demanding option, the bar plot in Figure 3 shows that the majority of participants (more than 50%) answering our post-interaction survey rated themselves as "very particular" or "particular" when sharing their private information.

This effect indicates that our social robot application was able to successfully maintain contextual integrity [28] for the majority of participants. We were able to match privacy expectations for appropriate information flows so users were comfortable selecting face identification, even if they self reported as at least "particular" regarding their privacy. However, it is important to mention that our participants were aware that their face information was being collected by experimenters from a public university conducting a research study and not for a commercial product. This factor may have reduced their privacy concerns towards the system [31], resulting in their decision to grant the robot permission to record their face information. In addition to that, it is important to note that face identification technologies are becoming more and more present in personal devices such as smartphones, tablet and laptops due to their easy, quick, effective and practical use [32]. This additional reason may further explain why a large majority of participants selected face identification. Indeed, by looking at Table V, the majority of the motivations provided explain the choice for face identification because of its convenience in term of ease-of-use, speed or accessibility. Besides that, novelty and curiosity also played a role in this choice. These results suggest that our participants were willing to give access to their private face information in exchange for an easier, quicker and more accessible login method; even if the system was not deployed on a personal device like a smartphone, but on a resource shared by visitors of a public space. Nonetheless, 18 out of 103 participants interacting with the robot (17.48%) did choose QR code. This option was a valid alternative to our system for users who may feel that providing their facial information was not within appropriate norms for information flow, motivating privacy concern. Only 7 participants (6.80%) out of a total of 103 users interacting with the robot left the registration process before completing it. Two of the three participants that selected QR code and completed the post-interaction survey motivated their choice due to a lack of trust in granting the system access to their face information. Without designing the QR code as a viable alternative, the number of people leaving the registration process may have risen to 24.27% (N. 18 + 7 out of 103 participants).

With respect to the number of participants completing both the two-step registration process (i.e. both robot and on-line registration), only 55 out of 99 participants (55.56%) who initiated and completed one of the steps required by the registration process (N. 3 from web + N. 96 from the robot) also completed the second step. Notably, none of the 3 users initiating the process from the on-line website completed the registration by visiting the robot on-site. Unfortunately, we did not have a large enough distribution of participants across groups to be able to make strong conclusions about any interaction between initiating the sign up from the on-line website vs robot and the completion of the registration process. However, our first results might suggest that when designing a cross-platform multi-step registration process for social robot applications, it is more effective to design an interaction flow that simply starts from the interaction with the robot. Our analysis within the much larger sample of users initiating and completing the registration process on the robot (N. 96) to examining the interactions between the chosen modality (i.e. face identification vs QR code) and the completion of the registration on-line was not significant. Therefore, we did not find evidence to suggest that the chosen access method leads to a significantly different number of participants completing the second step. From a design perspective, this result suggests that the access methods play little or no role in users completing the second part of the registration process.

Finally, from the comments collected we gathered a general positive sentiment towards the designed experience. The majority of adjectives used were positive and used in the participants' comments 20 out of 31 total times (64.25%). Pepper was mostly described with positive qualities and the physical appearance and design of the robot may have played a role in shaping an overall positive experience for our participants. Importantly, the majority of negative comments were suggesting a slow and long process to register with the robot. The interaction with the robot required a maximum of 5 minutes, during this time the robot communicated details of the data collection process and the login system via several steps. Usually, when designing a commercial product users are given control over acquiring details by means of a separate menu or button (i.e. 'disclaimer', 'more information' or 'how does it work?'). However, due to the experimental nature of our study we needed to make sure that every participant acquired the same amount of information. This lead to a longer interaction, requiring multiple steps and additional clicks on the robot's tablet to complete the registration process, but gave the necessary high level of transparency.

VIII. Limitations and Conclusions

This study required a considerable amount of work and several days in the field. However, this effort was compensated with a total of 106 real users and many important observations on human-robot interaction in the wild.

In this paper we limited our discussion to people's preferences when registering their identity to use a publicly available and shared social robot. We found that the majority of people were comfortable registering their face information to gain access to the available services, but that a non-trivial proportion of people were not at ease with doing so. As such, the designed alternative to face identification, i.e. the use of a QR code, played a critical role in increasing the number of users adopting the technology. This is an important contribution to the development of future social robot applications, as many potential use cases will require the permission of the user to store sensitive information and such systems should promote the inclusion of as many users as possible by offering viable registration alternatives. We demonstrated the importance of addressing privacy as the first step in the design of social robot applications and discussed how transparency crucially affects user trust. The reported results provide evidence that designing for privacy with inclusiveness and transparency upfront leads to responsible social robots applications that can be trusted by users and consequently adopted by the majority of the population.

The main limitation of our study is the nature of the designed system. Our participants knew the system was not a commercial application and that the collected data would be deleted after the completion of this study. This approach may have played a role in reducing people's privacy concern in registering their face due to their inherent trust of researchers from a public University constrained by ethics procedures [31]. In addition, during this first design iteration we mainly focused on the registration system. Although the robot was designed to provide valuable services for the situated context (e.g. facilitating meetings and collecting data for surveys designed by startup entrepreneurs), such services were not deployed at this stage. Instead, the robot only provided a few secondary services, such as telling jokes or allowing people to take selfies. This limitation may have played a role in reducing the proportion of participants that completed the two required registration steps. Finally, in this study we employed a Pepper robot. The interaction behaviour of users, as well as their sentiments towards the registration process, may differ with the use of different types of robots.

In our future studies we will consider further design iterations of the proposed robot application. In these iterations the robot will offer users more services specifically designed to meet their needs for the considered environment. We will investigate changes in users' behaviour and their preferences when registering with the robot to access its newly deployed services. In addition, we will gather data on users' overall experience when using such services.

References

[1] M. Joosse and V. Evers, "A guide robot at the airport: First impressions," in *Proceedings of the Companion of the 2017 ACM/IEEE International Conference on Human-Robot Interaction*. ACM, 2017, pp. 149–150.

[2] M. Tonkin, J. Vitale, S. Herse, M.-A. Williams, W. Judge, and X. Wang, "Design methodology for the ux of hri: A field study of a commercial social robot at an airport," in *Proceedings of the 2018 ACM/IEEE International Conference on Human-Robot Interaction*. ACM, 2018, pp. 407–415.

[3] T. Kanda, M. Shiomi, Z. Miyashita, H. Ishiguro, and N. Hagita, "An affective guide robot in a shopping mall," in *Proceedings of the 4th ACM/IEEE international conference on Human robot interaction*. ACM, 2009, pp. 173–180.

[4] M. Tonkin, J. Vitale, S. Ojha, M.-A. Williams, P. Fuller, W. Judge, and W. Xun, "Would you like to sample? robot engagement in a shopping centre," in *Proceedings of the 26th IEEE International Symposium on Robot and Human Interactive Communication (RO-MAN 2017)*. IEEE, Aug 2017, pp. 42–49.

[5] K. Kaipainen, A. Ahtinen, and A. Hiltunen, "Nice surprise, more present than a machine: Experiences evoked by a social robot for guidance and edutainment at a city service point," in *Proceedings of the 22nd International Academic Mindtrek Conference*. ACM, 2018, pp. 163–171.

[6] M. J.-Y. Chung and M. Cakmak, “how was your stay?: Exploring the use of robots for gathering customer feedback in the hospitality industry,” in *2018 27th IEEE International Symposium on Robot and Human Interactive Communication (RO-MAN)*. IEEE, 2018, pp. 947–954.

[7] R. Mead, D. H. Grollman, A. Lim, C. Yeung, A. Stout, and W. B. Knox, “Hri 2018 workshop: Social robots in the wild,” in *Companion of the 2018 ACM/IEEE International Conference on Human-Robot Interaction*, ser. HRI ’18. New York, NY, USA: ACM, 2018, pp. 399–400. [Online]. Available: http://doi.acm.org/10.1145/3173386.3173569

[8] C. L. Breazeal, *Designing sociable robots*. MIT press, 2004.

[9] M. Willis, “Human centered robotics: Designing valuable experiences for social robots,” in *Proceedings of HRI2018 Workshop (SocialRobots in the Wild)*, 2018.

[10] J. Vitale, M. Tonkin, X. Wang, S. Ojha, M.-A. Williams, and W. Judge, “Privacy by design in machine learning data collection: A user experience experimentation,” in *Symposium on Designing the User Experience of Machine Learning Systems*. AAAI Spring Symposia 2017, 2017, pp. 439–442.

[11] M. Tonkin, J. Vitale, S. Ojha, J. Clark, S. Pfeiffer, W. Judge, X. Wang, and M.-A. Williams, “Embodiment, privacy and social robots: May i remember you?” in *International Conference on Social Robotics*. Springer, 2017, pp. 506–515.

[12] J. Vitale, M. Tonkin, S. Herse, S. Ojha, J. Clark, M.-A. Williams, X. Wang, and W. Judge, “Be more transparent and users will like you: A robot privacy and user experience design experiment,” in *Proceedings of the 2018 ACM/IEEE International Conference on Human-Robot Interaction*. ACM, 2018, pp. 379–387.

[13] M. A. Glendon, “Knowing the universal declaration of human rights,” *Notre Dame L. Rev.*, vol. 73, p. 1153, 1997.

[14] M. R. Calo, “Robots and privacy,” in *Robot Ethics: The Ethical and Social Implications of Robotics*, P. Lin, K. Abney, and G. A. Bekey, Eds. The MIT Press, 2011, ch. 12, p. 187.

[15] M. Rueben, C. M. Grimm, F. J. Bernieri, and W. D. Smart, “A taxonomy of privacy constructs for privacy-sensitive robotics,” *arXiv preprint arXiv:1701.00841*, 2017.

[16] M. Rueben, W. D. Smart, C. M. Grimm, and M. Cakmak, “Privacy-sensitive robotics,” in *Proceedings of the Companion of the 2017 ACM/IEEE International Conference on Human-Robot Interaction*. ACM, 2017, pp. 425–426.

[17] Y. Welinder and A. Palmer, “Face recognition, real-time identification, and beyond,” in *The Cambridge Handbook of Consumer Privacy*, E. Selinger, J. Polonetsky, and O. Tene, Eds. Cam-

bridge University Press, 2018, ch. 7, pp. 102–124.

[18] M. J. Culnan and P. J. Bruening, "Privacy notices: Limitations, challenges, and opportunities," in *The Cambridge Handbook of Consumer Privacy*, E. Selinger, J. Polonetsky, and O. Tene, Eds. Cambridge University Press, 2018, ch. 29, pp. 524–545.

[19] N. Richards and W. Hartzog, "Taking trust seriously in privacy law,(2016)," *Stanford Technology Law Review*, vol. 19, p. 431, 2019.

[20] A. K. Schnackenberg and E. C. Tomlinson, "Organizational transparency: A new perspective on managing trust in organization-stakeholder relationships," *Journal of Management*, vol. 42, no. 7, pp. 1784–1810, 2016.

[21] M. J. Culnan and R. J. Bies, "Consumer privacy: Balancing economic and justice considerations," *Journal of social issues*, vol. 59, no. 2, pp. 323–342, 2003.

[22] S. Herse, J. Vitale, M. Tonkin, D. Ebrahimian, S. Ojha, B. Johnston, W. Judge, and M.-A. Williams, "Do you trust me, blindly? factors influencing trust towards a robot recommender system," in *2018 27th IEEE International Symposium on Robot and Human Interactive Communication (RO-MAN)*. IEEE, 2018, pp. 7–14.

[23] M. J. Culnan and C. C. Williams, "How ethics can enhance organizational privacy: lessons from the choicepoint and tjx data breaches," *Mis Quarterly*, pp. 673–687, 2009.

[24] A. Freedy, E. DeVisser, G. Weltman, and N. Coeyman, "Measurement of trust in human-robot collaboration," in *2007 International Symposium on Collaborative Technologies and Systems*. IEEE, 2007, pp. 106–114.

[25] M. König and L. Neumayr, "Users resistance towards radical innovations: The case of the self-driving car," *Transportation research part F: traffic psychology and behaviour*, vol. 44, pp. 42–52, 2017.

[26] D. F. Glas, S. Satake, F. Ferreri, T. Kanda, N. Hagita, and H. Ishiguro, "The network robot system: Enabling social human-robot interaction in public spaces," *J. Hum.-Robot Interact.*, vol. 1, no. 2, pp. 5–32, Jan. 2013. [Online]. Available: https://doi.org/10.5898/JHRI.1.2.Glas

[27] L. Fiorini, R. Esposito, M. Bonaccorsi, C. Petrazzuolo, F. Saponara, R. Giannantonio, G. D. Petris, P. Dario, and F. Cavallo, "Enabling personalised medical support for chronic disease management through a hybrid robot-cloud approach," *Autonomous Robots*, vol. 41, no. 5, pp. 1263–1276, Jun 2017.

[28] H. Nissenbaum, *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press, 2009.

[29] P. Kumaraguru and L. F. Cranor, *Privacy indexes: a survey of Westin's studies*. Carnegie Mellon University, School of Computer Science, Institute for , 2005.

[30] G. Danezis, J. Domingo-Ferrer, M. Hansen, J.-H. Hoepman, D. L. Metayer, R. Tirtea, and S. Schiffner, "Privacy and data protection by design – from policy to engineering," *European Union Agency for Network and Information Security (ENISA)*, 2014.

[31] K. Martin and H. Nissenbaum, "Measuring privacy: an empirical test using context to expose confounding variables," *Colum. Sci. & Tech. L. Rev.*, vol. 18, p. 176, 2016.

[32] E. Vazquez-Fernandez and D. Gonzalez-Jimenez, "Face recognition for authentication on mobile devices," *Image and Vision Computing*, vol. 55, pp. 31–33, 2016.