Be More Transparent and Users Will Like You: A Robot Privacy and User Experience Design Experiment

Jonathan Vitale
University of Technology Sydney
Centre for Artificial Intelligence
The Magic Lab
jonathan.vitale@uts.edu.au

Meg Tonkin
University of Technology Sydney
Centre for Artificial Intelligence
The Magic Lab
margaret.tonkin@student.uts.edu.au

Sarita Herse
University of Technology Sydney
Centre for Artificial Intelligence
The Magic Lab
sarita.herse@student.uts.edu.au

Suman Ojha
University of Technology Sydney
Centre for Artificial Intelligence
The Magic Lab
suman.ojha@student.uts.edu.au

Jesse Clark
University of Technology Sydney
Centre for Artificial Intelligence
The Magic Lab
jesse.clark@uts.edu.au

Mary-Anne Williams
University of Technology Sydney
Centre for Artificial Intelligence
The Magic Lab
Mary-Anne@themagiclab.org

Xun Wang
Commonwealth Bank Australia
Innovation Lab
Xun.Wang@cba.com.au

William Judge
Commonwealth Bank Australia
Innovation Lab
william.judge@cba.com.au

ABSTRACT

Robots interacting with humans in public spaces often need to collect users' private information in order to provide the required services. Current privacy legislation in major jurisdictions require organisations to disclose information about their data collection process and obtain user's consent prior to collecting privacy sensitive information. In this study, we considers a privacy-sensitive design of a data collection system for face identification. We deployed a face enrolment system on a humanoid robot with human like gesturing and speech. We compared it with an equivalent system, in terms of capability and interactive process, on a screen-based interactive kiosk. In our previous contribution, we investigated the effects that embodiment has on users' privacy considerations. We found that an embodied humanoid robot is capable of collecting more private information from users as compared to a disembodied interactive kiosk. However, this effect was statistically significant only when the two compared systems were using a transparent interface, *i.e.* an interface communicating to users the privacy policies for data processing and storage. Thus, in this work, we aim to further investigate the effects of transparency on users' privacy considerations and their experience with the system. We found that when comparing a non-transparent *vs.* transparent interface within the same system (*i.e.* on an embodied robot or on a dis-embodied kiosk) transparency does not lead to significant effects on users' privacy considerations. However, we found that transparency leads to a significantly better user experience for both systems. Therefore, our overall analyses suggest that, while both the robotic system and the interactive kiosk are capable of enhancing the user experience by providing transparent information to users, which is required by privacy legislation, the interactive kiosk pays this feature by eliciting more privacy concerns in users compared to the robotic system. This exploratory study provides conclusions able to provide valuable insights for designing robotic applications dealing with users privacy and it discusses the related legal implications, concluding with few recommendations for privacy policymakers.

CCS CONCEPTS

• **Security and privacy → Usability in security and privacy**; *Social aspects of security and privacy*; • **Human-centered computing →** *Empirical studies in interaction design*; • **Computer systems organization →** *External interfaces for robotics*;

KEYWORDS

privacy-sensitive design, human-robot interaction, User Experience design, privacy considerations, transparency

ACM Reference format:
Jonathan Vitale, Meg Tonkin, Sarita Herse, Suman Ojha, Jesse Clark, Mary-Anne Williams, Xun Wang, and William Judge. 2018. Be More Transparent and Users Will Like You: A Robot Privacy and User Experience Design Experiment. In *Proceedings of ACM International Conference on Human-Robot Interaction, Chicago, Illinois USA, March 2018 (HRI2018),* 9 pages.
https://doi.org/10.475/123_4

HRI2018, March 2018, Chicago, Illinois USA

ACM ISBN 123-4567-24-567/08/06…$15.00
https://doi.org/10.475/123_4

1 INTRODUCTION

Robots providing services in public spaces are commonly asked to engage and entertain customers [9, 16, 26]. To achieve a sufficient level of social skills, the robots needs to access users' private information, like their facial features, identity, preferences and so on [20, 22]. As an example, collecting the identity of customers can be a valuable information to increase the robot's social intelligence and enhance the user experience in future interactions; in fact, the

robot can appropriately tailor the dialog and provide a best service by taking into account the customer's known information [22].

Current privacy legislation requires to disclose enough information to users about the data collection process and give them options for choosing if releasing or not their sensitive information [17, 18]. Adhering to these principles is imperative. For example, in 2018 the European Union General Data Protection Regulation 679/2016 will be binding and it will include sanctions up to criminal charges for systems not ensuring a proper level of privacy [23].

Prior collection of user's information a system must provide sufficiently transparent information to the users to allow them (i) accessing the organisation's privacy policy with references to the country current legislation and user's rights and (ii) gathering any information on how the private data is processed, stored, used and possibly shared by the system [17]. Here it is important to remind that *systems not adhering to these privacy principles are illegal*. In this paper, we define the term *transparency* in relation to the clarity of the information provided by a system to an individual about the collection, processing, storage, usage and sharing of his private information when interacting with the considered system [23, refer to art. 12].

We argue that it is important to *understand how disclosing transparent information to users affects their privacy considerations, potentially biases their decisions, and influences their user experience*. Gathering insights around this topic will advance investigating the validity of the following hypotheses:

Hypothesis 1 (H1): *A transparent system increases users' risk tolerance when asking for their private information, thus reducing user's privacy concerns and significantly increasing the quantity of collected private information, as compared to a non-transparent system.*

Hypothesis 2 (H2): *A transparent system leads to a better understanding of the system and, consequently, to a significantly more positive user experience as compared to a non-transparent system.*

We assess the validity of these hypotheses by analysing and discussing data collected during a recent privacy experiment [25]. This recent work investigated a face enrolment system adopted to remember participants identities when interacting with the digital services provided by the company research lab during their future visits. It was shown that, when using an interface disclosing information to users about the data collection process (*i.e.* transparent interface), people released significantly more private information when interacting with an embodied gesturing and speaking humanoid robot, as compared to a disembodied interactive kiosk made up of a tablet connected to a webcam. However, this effect was not found significant when comparing the two systems using a non-transparent interface, namely an interface not disclosing enough privacy information to users. Hence, in this work, we deepen our investigation on *transparency* by considering its effects on users' privacy considerations and by extending the analyses to its impact on users' experience within the two considered systems.

An important original contribution of this work is the unification of privacy research with User Experience Design (UX). Our approach draws inspiration from *privacy by design* and we refer to it as a *privacy-sensitive* approach [13, 17, 19, 28, 29]. A privacy-sensitive design approach ensures privacy protections are introduced at the beginning of system design, rather than being tacked on at the end. This is particularly important when designing commercial robot applications in real-world human-centric business environments [24, 29]. Indeed, existing systems built without including privacy considerations as a core part of their development often result in poor privacy management and a lack of use adoption [29]. This may be experienced as a disparity between stated privacy policies and actual privacy controls [2]. In addition, the findings of our study can benefit privacy policymakers to provide legislative tools to better protect the privacy of users in the particular context of robotic systems.

2 TRANSPARENCY, PRIVACY AND USER EXPERIENCE

Privacy issues that arise in real-time data collection can be addressed explicitly, by providing specific guidelines aimed at reducing the amount of sensitive data stored in a system [6] or by using encryption algorithms to safely store collected data [3].

In addition, privacy can be implicitly addressed by a machine learning algorithm itself. For instance, an algorithm can learn which features to extract from inputs after a training phase. This new representation is then extracted from new observations in order to classify them with competitive recognition rates. However, the extracted features might not contain enough information for reconstructing the original input [1], thus relieving privacy concerns. Despite these important precautions, the majority of naïve users do not know the underlying details of the machine learning algorithm used, what data would be stored by the system, and how. This lack of *transparency* can lead to privacy concerns and to violation of privacy laws [17, 18, 23].

Effects of information transparency on privacy concerns and trust towards the system have been previously investigated. Wu and colleagues found that the way the online privacy policy is presented to users significantly affects their *privacy concerns*, and that this in turn influences users' trust [31]. In line with this, other researchers also concluded that disclosing information handling practices of a company helps to reduce privacy concerns [4, 14], which in turn improves the *trust* of the individual towards the system [8] and enhances the *willingness to provide personal information* [5, 31].

Previous research supports the fact that transparency of a system has an effect on a user's experience in using a system. For example, Sinha and Swearingen [21] found that a recommender system which explains the mechanism involved in the process of making a particular decision is liked more by the users and users experience a feeling of more confidence in following a recommendation given by such a system as compared to less transparent one [21]. Additionally, Konstan and Riedl stress that increased transparency of explanation of underlying mechanism helps to improve user experience in recommender systems [11]. The literature suggests that mostly the role of transparency in user experience design has been conducted in settings of recommender systems [11, 21] or non-humanoid robots [30] solely.

Therefore, we identified a major gap of current literature on studying the effects of transparency in embodied robotic systems

and, contrary to previous literature, our work situates the experiment on a face enrolment system available in the innovation lab of a bank designed to provide digital services for its customers and employees.

One of the few works investigating transparency for robotic technologies is that by Kin and Hinds [10]. In it the authors explored the effect of transparency on the tendency to blame a robot, the self or other participants. Although this work investigated transparency for a robotic application, it did not investigate the effects transparency has on privacy and user experience.

Thus, a major novel contribution of our paper is the provision of a more comprehensive understanding of transparency for robotics applications by investigating effects on both privacy and user experience within a single experimental study. With this work we aim to foster the growing interest in privacy-sensitive robotics research that focuses on the deployment of real robots in commercial applications [19].

3 METHOD

We situated our experiment in the Innovation Lab of Commonwealth Bank of Australia where the bank undertakes user experiments with new technologies before deployment. This lab focuses on studying and developing innovative products and services in collaboration with customers, partners, startups and industry.

One of the primary steps necessary to demonstrate proficiency in social intelligence is knowing people, which involves memorising human identities so they can be recognised again at a later date, therefore facilitating social exchanges [7]. In digital systems, this task involves the recording of sensitive user's information, thereby creating an optimal use case to frame our investigation on privacy.

3.1 Robot Platform

The humanoid robot used in this experiment has been adopted since August 2016 to explore and identify opportunities for potential future commercial applications for bank customers including shopping centres and airports [24, 26].

The robot platform used in this experiment is a REEM robot[1] a wheel-based human-sized humanoid robot equipped with a pair of stereo cameras on its head (for eyes). The robot has a pair of 7-degrees of freedom (DOF) arms and 3-DOF hands that can perform human-like gestures. Built into the front of the robot at chest height is a touch screen, which is used during the experiment to display the Graphic User Interface (GUI) of the face enrolment system under investigation. The robot communicated with the user through gestures, speech, and text on its monitor.

3.2 Experimental Design

In this study we considered two independent binary variables: *embodiment* (*i.e.* either embodied or disembodied) and *transparency* (*i.e.* either transparent or not transparent), thus leading to a 2×2 between-subjects design.

Embodied and disembodied conditions. During the embodiment conditions the participants interacted with the humanoid robot through the monitor integrated in its chest. The text of the GUI was simultaneously acted through the robot speech and gestures.

During the disembodied conditions the participants interacted with an interactive kiosk, namely a tablet connected to a webcam. The tablet has the same dimensions as the robot's monitor and it was situated at the same height. The webcam was placed at the same height of the robot's cameras (Figure 1). The graphical user interface used on the tablet was exactly the same as the one used on the robot's monitor, with the only difference being that the text was not acted through speech and gestures.

Transparent and non-transparent conditions. The transparent conditions differed from the non-transparent conditions by including additional stages of the face enrolment interface informing the user about the face recognition algorithm used, how the data was recorded and stored, and legal privacy policies followed by the bank to store the private information. In the transparent condition, this information was communicated after the welcoming interface and right before asking the user's consent to proceed.

In this study we pretended to record the user's facial features. Thus no users' private information was actually collected throughout the experiment. However, in order to elicit users' privacy considerations, the interface signalled the intention to collect their private information in all the considered experimental conditions from the first screen presented to the user (see section 3.5 for a summary of the user interface flow).

3.3 Participants

Participants were invited to join our experiment via e-mail sent to 'friends of the lab', namely a mailing list of staff, students and visitors of the bank innovation lab. We included in our study a population proficient in English reading and listening, and balanced in terms of computer literacy.

A total of 84 people expressed the intention to participate in the experiment. However, in a post-experiment questionnaire we asked which social networks accounts the participants used. Since in our experimental methodology we used Facebook to elicit user privacy considerations, we discarded 9 participants not owning a Facebook account from the study. We also excluded 3 additional subjects due to technical issues preventing the user consent data recording, thus leading to a total of 72 participants (41 males and 31 females, ranging from 18 to 60 years old).

Each participant was randomly allocated to one of the four experimental conditions as summarised by Table 1.

Table 1: Number of Participants allocated to the 4 different experimental conditions

	Embodied	**Dis-Embodied**	***Total***
Transparent	21 (29%)	20 (28%)	41 (57%)
Non-Transparent	15 (21%)	16 (22%)	31 (43%)
Total	36 (50%)	36 (50%)	72 (100%)

3.4 Procedure

The experiment included three main stages: (1) an introduction of the experiment to the participants together with a pre-experiment

[1] http://pal-robotics.com/wp-content/uploads/2016/03/REEM-Datasheet.pdf

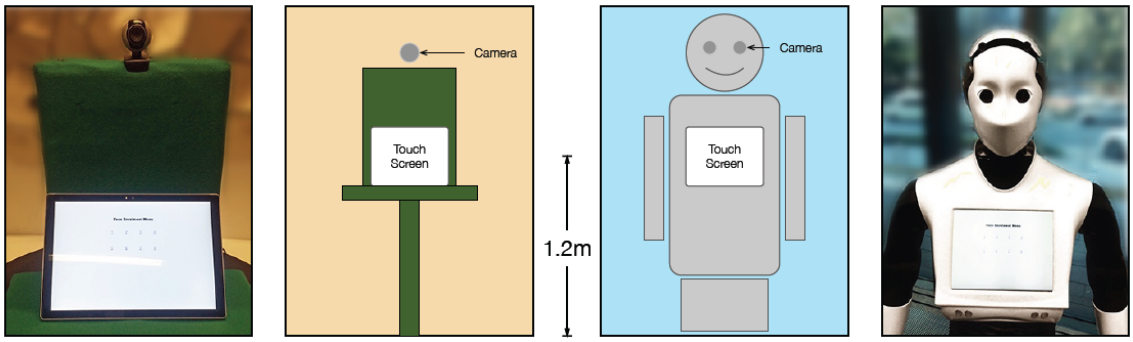

Figure 1: Face enrolment setup on the REEM robot and the alternative disembodied setup on a kiosk-like setup.

questionnaire (to collect data like gender and age group) and a quick tour of the labs; (2) the interaction with the face enrolment system in one of the considered four settings; (3) a post-experiment questionnaire evaluating the participants' user experience.

3.5 Face Enrolment System User Interface

The user interface of the system started with a **welcome page** providing the following message: "We would like to take your photo so we can welcome you back next time you visit". This screen was common to all the experimental conditions and necessary to signal to the users the intention of collecting their private information.

After this welcome page, if the participant was in the non-transparent condition, the system directly proceeded with the **user consent page**. This screen provided the following message: "Can we remember your face to greet you next time you visit? *[button NO] [button YES]*".

In the alternative case of the transparent condition, before asking for user consent the system provided information about data processing and storage, and the privacy policy through a set of **transparency pages**. The user was provided the following information: "We can take a photo of your face, and convert your features to the equivalent of a digital pin. Something like this *[it follows an image of a face and a long sequence of corresponding numbers]*. We store these numbers, not your actual photo, and keep them securely in our database. The numbers cannot be used to recreate your photo. Only we can use the numbers to recognise you next time you come to visit. We do not share your information with anyone and will only use it to greet you. Our privacy policy can be viewed at anytime online at *[it follows a url]*."

If the user consented to proceed the **snapshot page** was presented showing a countdown of 10 seconds together with video camera feedback. The feedback was necessary to show the users that the camera was recording their faces and therefore simulating a real data collection. Nonetheless, we did not actually take any picture of the participants. In the case the user did not provide the consent the concluding page was shown and the experiment terminated.

If the experiment proceeded, the system presented the **participant name page** asking the participant for their name through an input textbox and providing the following message: "Could you tell me your name?".

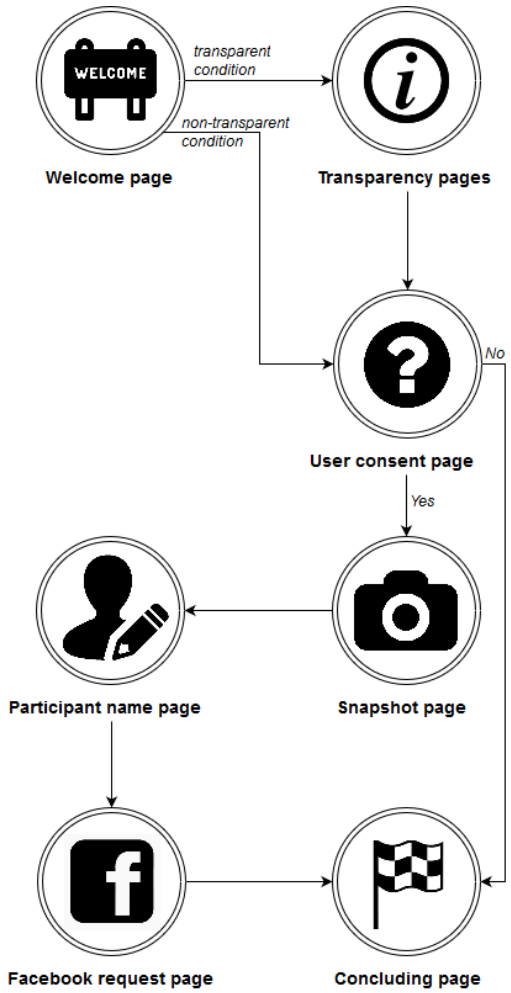

Figure 2: The user interface flow of the face enrolment system.

From previous pilot experiments and surveys [28] we knew that asking participants to record their face is not enough to elicit privacy considerations and detect effects on privacy in the considered

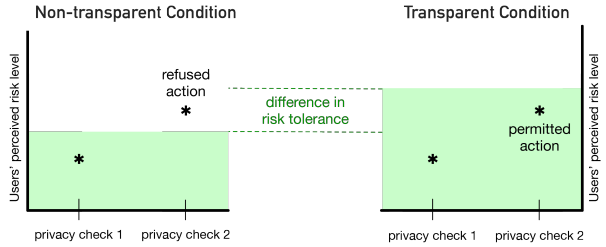

Figure 3: Visual explanation of our hypothesis: compared to a non-transparent interface, the transparent one would increase users' risk tolerance "comfort zone" when asking for private information, thus reducing users' privacy concerns and consequently collecting, on average, more positive answers during the two privacy checks.

context (see section 3.6 for a discussion). On the contrary, our previous pilot studies showed that asking users to connect to their Facebook accounts was assessed as an inappropriate intrusion of users' privacy in this context. Therefore, we included in the interface an additional **Facebook request page** asking user's consent for connecting to the Facebook account of the participant: "Thank you [input name]. It's nice to meet you! Let's stay in touch by connecting on Facebook. Is that okay with you? *[button NO] [button YES]*". This second privacy check was used as a more powerful way to elicit users' privacy concerns, therefore better detecting effects on privacy, as we will discuss later in section 3.6.

Finally, the experiment ended when the system displayed the **concluding page** by saying: "Okay! See you next time!". This message was common for all four experimental conditions and for any answer given by the user (either agree to consent or disagree).

Figure 2 provides a summary of the user interface flow for all four conditions of the experiment.

3.6 Measures

3.6.1 Privacy Measurements. Normally, requiring users to record their facial features may elicit privacy concerns. However, financial institutions are usually perceived as reliable organisations by users in safely storing their personal information [27]. In addition, many large organisations, such as banks, already ask their employees to release their biometric information (*e.g.* photo ID, fingerprints, face biometrics, *etc.*). Hence, asking participants to memorise their face together with simple additional private information (*e.g.* name, address, telephone number, *etc.*) may not be perceived as a risk, thus not rising sufficient privacy concerns by users.

To test this hypothesis we conducted a preliminary survey among 282 people (bank staff, customers, students) [28]. We discovered that a robot collecting information such as name, address and phone number was considered to be 'okay' 36.82%, or 'definitely okay' 20.94%, in a bank. In addition, we expected that by asking the users to provide access to their social networks accounts would be perceived as an intrusion outside the normal boundaries perceived appropriate for a bank institution. Indeed in our same survey, only 8.96% of users expressed to be 'okay' and 4.48% 'definitely okay' with the robot in a bank asking to connect to social networks.

Therefore, in this experiment we obtained an indirect measurement of users' privacy concerns by means of two privacy checks.

- The first privacy check counted how many users consented to take a photo of their face and it was aligned with what expected to find in the working prototype of the designed face enrolment system.
- The second privacy check counted the number of participants who agreed to connect with the face enrolment system to their Facebook account.

The second privacy check provides a higher threshold than the first privacy check and allows us to measure the impact of the UX on a participants privacy tolerance during the face enrolment experiment.

We believe that transparent and non-transparent conditions would set a certain risk tolerance "comfort zones" in the participants. Therefore, assuming that the two privacy requests would be perceived by the participants, on average, with a certain level of risk, we suggest that during the transparent condition the risk tolerance would be higher compared to the non-transparent condition where the participant would not have any reassurance about how the data would be stored and managed by the organisation. Hence, we predict to observe less privacy concerns and, consequently, a more positive user experience in the transparent settings compared to the non-transparent ones. This hypothesis is visually explained by Figure 3.

The considered methodology for measuring effects on privacy in users is inspired by the first three principles of Krol *et al.* regarding robust experimental design for security and privacy [12, page 21]: *"(i) give participants a primary task; (ii) incorporate realistic risk; (iii) avoid priming the participants"* and extensively justified by recent contributions and appropriate manipulation checks [25].

3.6.2 Reaction Times. We measured the participants reaction time of taking a decision to agree or disagree to providing access to their private information. This measurement was taken on both user consent pages for both the face recording and Facebook connection request. With these measures we want to investigate if there are significant differences in time reactions during these decisions and, consequently, delays due to additional cognitive loads possibly caused by further privacy concerns when taking a decision on if sharing or not private information.

3.6.3 User Experience Measurements. For measuring the user experience of the considered system we used the User Experience Questionnaire (UEQ) by Laugwitz, Held and Schrepp [15][2].

This questionnaire consists of 24 pairs of contrasting qualities that participants should judge with regards to the experienced face enrolment system. The qualities are scored by gradations between opposites on seven-steps Likert scales. The seven-step scale was used to reduce the central tendency bias for such items.

The considered qualities are organised into six groups: Attractiveness (*e.g.* good/bad, annoying/enjoyable), Perspicuity (*e.g.* complicated/easy, not understandable/understandable), Efficiency (*e.g.* fast/slow, organised/cluttered), Dependability (*e.g.* unpredictable/

[2] Please refer to http://www.ueq-online.org/ for related details and data analysis tools.

predictable, secure/not secure), Novelty (*e.g.* creative/dull, conservative/innovative) and Stimulation (*e.g.* motivating/demotivating, boring/exciting).

We administered the UEQ to the participants after the interaction with the face enrolment system via a portable iPad.

4 RESULTS

We set the significant level to an alpha equal to 0.05. For the considered analyses we used the software Minitab[3].

4.1 Analysis of User Consent

We recorded the number of participants who agreed to having a photo of their face taken by the robot or kiosk with respect to the total number of participants in each condition. Among the participants giving their consent to proceed with the face enrolment process, we recorded the number of users providing their consent to connect to their Facebook account. These measurements returned the proportions of users giving their consent during the first and second privacy check. Table 2 summarises the number of participants providing their consent to enrol their face, as well as the number of participants accepting the Facebook connection request after giving consent to proceed with the face enrolment process.

Table 2: Summary of the participants who gave their consent to enrol their face in the system and accepted the Facebook request.

Face enrolment	**disembodied**	**Embodied**
non-transparent	16/16 (100%)	14/15 (93.33%)
transparent	18/20 (90%)	21/21 (100%)
Facebook request	**disembodied**	**Embodied**
non-transparent	7/16 (43.75%)	8/14 (57.14%)
transparent	4/18 (22.22%)	11/21 (52.38%)

We used a z-test for two samples proportions to identify significant differences among transparent and non-transparent settings when controlling for embodiment type. We did not find significant differences in the number of people giving consent to enrol their face when comparing transparent and non-transparent conditions and controlling for embodiment type (dis-embodied condition: Z = 1.49; p = .136; embodied condition: Z = -1.04; p = .301). Similarly, we did not find significant differences in the number of people giving consent to connect to their Facebook account when comparing transparent and non-transparent conditions and controlling for embodiment type (dis-embodied condition: Z = 1.36; p = .173; embodied condition: 0.28; p = .781). It is important to report also our previous analyses [25] that found a significant effect during the second privacy check (*i.e.* Facebook consent) when comparing embodied and dis-embodied systems displaying a transparent interface (Z = -2.06; p = .040), but not when the two systems displayed a non-transparent interface (Z = -0.74; p = .460).

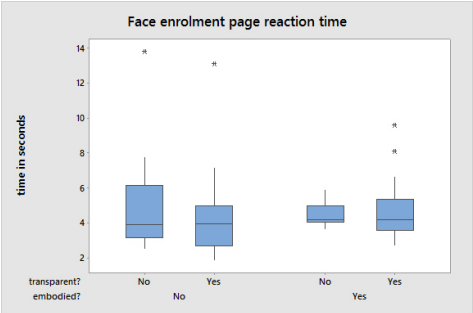

Figure 4: The reaction time (seconds) on the page asking users the consent to take their faces.

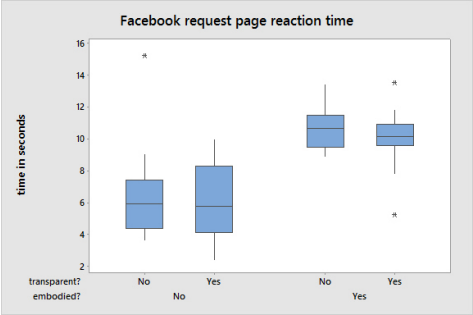

Figure 5: The reaction time (seconds) on the page asking users the connect to their Facebook account.

4.2 Analysis of Reaction Times

We recorded the reaction time of participants on the user consent page and the Facebook request page before making a decision of either agree or disagree to the face enrolment system requests. These were measured automatically by the system interface in seconds. Technical difficulties prevented the recording on the physical drive of the reaction time for three participants during the embodied-transparent condition. Thus, we excluded these participants from this analysis. We used a two-way ANOVA to compare the differences in means for the reaction times among the two considered factors: embodied/disembodied and transparent/non-transparent.

Figure 4 shows the reaction times among the four different conditions for the user consent page, whereas Figure 5 shows the reaction times for the Facebook request page. Whereas for the user consent page there are no noticeable differences between conditions, for the Facebook request page there is a dramatic increase in the reaction times during the embodied settings compared to the disembodied ones. Indeed, when considering the reaction times on the user consent page, we did not find main effects for both embodiment ($F(1,65) = 0.05$, $p = .820$) and transparency ($F(1,65) = 0.02$, $p = .885$). Similarly, no interactions effects were found ($F(1,65) = 0.42$, $p = .518$). However, when considering the reaction times on the Facebook request page, we found a main effect for embodiment ($F(1,62) = 61.31$, $p < .001$) but no effects on transparency ($F(1,62) = 0.53$, $p = .469$) or factors interaction ($F(1,62) = 0.09$, $p = .767$).

[3]http://www.minitab.com

Table 3: Summary of the follow-up univariate ANOVA analyses on each UX dimension.

	Embodiment				Transparency				Interactions					
UX dimensions	M_d	M_e	F(1,68)	P	M_n	M_t	F(1,68)	P	M_{dn}	M_{dt}	M_{en}	M_{et}	F(1,68)	P
Attractiveness	1.032	1.532	5.32	**.024***	0.990	1.504	4.34	**.041***	0.500	1.458	1.512	1.547	3.73	.058
Perspicuity	2.146	2.292	0.44	.510	2.121	2.293	0.95	.333	2.156	2.138	2.083	2.440	1.17	.283
Efficiency	1.410	0.931	2.90	.093	1.290	1.079	0.73	.395	1.234	$1.550^{\dagger a}$	1.350	$0.63^{\dagger b}$	4.81	**.032***
Dependability	0.660	1.069	3.64	.060	0.556	1.098	6.25	**.015***	0.328	0.925	0.800	1.262	0.10	.751
Stimulation	0.542	1.319	14.03	**.000*****	0.573	1.201	6.73	**.012***	$-0.219^{\dagger a}$	$1.1500^{\dagger b}$	$1.417^{\dagger b}$	$1.250^{\dagger b}$	10.98	**.001*****
Novelty	0.160	0.931	9.85	**.003****	0.137	0.854	6.03	**.017***	$-0.734^{\dagger a}$	$0.875^{\dagger b}$	1.067	$0.833^{\dagger b}$	10.81	**.002****

Notes: M_d, M_e, M_n, M_t, M_{dn}, M_{dt}, M_{en}, M_{et} are the means during the different experiment conditions. The subscript letters d, e, n and t stand respectively for dis-embodied, embodied, non-transparent and transparent. *p < .05, **p ≤ .01, ***p ≤ .001. † denotes significant differences by mean of a Tukey *post hoc* test between items having different letters.

The main effect for embodiment cannot be explained by a different duration of the interaction between the two considered technologies; in fact, we did not detect any main effect on the user consent page, which presented an interface and robot speech/gesturing quite similar to the one presented for the Facebook request page (see section 3.5 for a description of the interfaces).

4.3 Analysis of User Experience

We processed the data collected by the UEQ questionnaire with the tools provided by the authors of the questionnaire [15][4], thus obtaining transformed data for each questionnaire's item and the scale means per person of the six considered questionnaire's dimensions. We use these six responses as dependent variables for our statistical analyses.

An initial MANOVA analysis examined the six questionnaire dimensions as dependent variables, and embodiment and transparency as independent variables. The analysis showed a main effect for embodiment in user experience between robot and interactive kiosk (F(5, 64) = 6.457, p < .001; Wilk's λ = .665, η^2 = .34), a main effect for transparency (F(5, 64) = 3.169, p = .012; Wilk's λ = .802, η^2 = .20) and an interaction effect (F(5, 64) = 3.517, p = .007; Wilk's λ = .785, η^2 = .22).

We further investigated the differences in means for the six UX dimensions (Attractiveness, Perspicuity, Efficiency, Dependability, Stimulation, Novelty) within the two considered factors by mean of follow-up univariate ANOVA analyses. Table 3 summarises the results of these analyses. Specifically, we found that the embodied system was judged significantly more attractive (F(1,68) = 5.32, p = .024), stimulating (F(1,68) = 14.03, p = .000) and novel (F(1,68) = 9.85, p = .003) than the dis-embodied system. In addition, we found that the transparent interface was judged significantly more attractive (F(1,68) = 4.34, p = .041), dependable (F(1,68) = 6.25, p = .015), stimulating (F(1,68) = 6.73, p = .012) and novel (F(1,68) = 6.03, p = .017) than the non-transparent interface.

Finally, we detected interaction effects for efficiency (F(1,68) = 4.81, p = .032), stimulation (F(1,68) = 10.98, p = .001) and novelty (F(1,68) = 10.81, p = .002). A Tukey *post hoc* test revealed that the embodied transparent system was judged significantly less efficient compared to the disembodied transparent system (p = .021), whereas the disembodied non-transparent system was judged significantly less stimulative compared to the embodied transparent system (p = .000), to the embodied non-transparent system (p = .000), and to the disembodied transparent system (p = .000). Tukey test revealed also that the disembodied non-transparent system was again judged significantly less novel compared to the embodied transparent system (p = .001), to the embodied non-transparent system p = .000), and to the disembodied transparent system (p = .001).

[4]See footnote 2.

5 GENERAL DISCUSSION

From our analyses we found that **there is no sufficient evidence to validate hypothesis H1**. In fact, when comparing the transparent and not-transparent interfaces withing the same system (*i.e.* robot or kiosk), there are no significant differences in the number of private information collected by that system. Similarly, when considering the time spent by users on the user consent and Facebook consent pages we found only a main effect for embodiment in the Facebook consent page, but no effects for transparency or interaction effects. These are interesting results. In fact, in our previous analyses we found that an embodied robot using a transparent interface can collect significantly more users' private information than a kiosk using the very same transparent interface, but this effect is not significant when the two systems use the non-transparent interface [25]. Hence, here we suggest that the presence or not of transparent information on the system's interface is not the crucial feature impacting on users' privacy considerations. Indeed, it is the design of the system that leads to major differences in users' privacy considerations, at least in this considered scenario and application. A system having a humanoid form and human-like capabilities, such as speech and gestures, can alter the risk perception of users and facilitate the collection of more private information compared to a dis-embodied system [25]. Nevertheless, this effect is only visible when the systems under comparison are providing transparent information, as required by privacy legislation.

Our analyses on user experience data **provide strong evidence in support of our second hypothesis (H2)**, namely that a transparent system leads to a more positive user experience, as compared to a non-transparent system. In fact, we found a main effect on transparency for the six dimensions of user experience considered as a whole. By further investigating the data with follow-up univariate ANOVA analyses, we found that transparency positively impacts on the perceived attractiveness, dependability, stimulation and novelty of the system. We did not find effects for perspicuity and efficiency. Detecting an effect for dependability dimension is particularly important for our study. In fact, this measure of user experience is related with items investigating security and predictability of the

system, which is aligned with our predictions that providing additional information to users facilitates a better understanding of the system and has a positive impact on their user experience. The lack of main effects for perspicuity was not a surprise, since the ease of use for both transparent and non-transparent interfaces was not manipulated and the interactions required for both the robot and the interactive kiosk were the same, namely tapping on a touchscreen display. We can speculate that the transparent interface, since providing additional information on how the face enrolment application recorded the faces to näive users, may have been perceived as more attractive, stimulating and novel, as compared to the non-transparent interface. Finally, we found interesting that when the robotic system provided transparent information was perceived less efficient then an interactive kiosk providing the same transparent information. We can speculate that this effect was due to a different touch sensitivity of the robot display as compared to the kiosk touchscreen. In fact, during the debriefing interviews, some of the participants suggested that the robot monitor was not reactive enough. This factor together with the additional number of pages, and therefore taps, required by the transparent interface may have significantly affected the perceived efficiency of the embodied transparent system as compared to the disembodied transparent one.

In the perspective of a privacy-sensitive design approach, being able to detect these effects is particularly crucial, since users' privacy considerations are considered an essential element to which paying attention when designing the UX of the considered system [19].

6 LEGAL IMPLICATIONS OF THE FINDINGS

Our study opens an important discussion around the topic of current privacy legislation. Firstly, we were able to demonstrate that the provision of transparent information to users required by law does not significantly affect users' privacy considerations. We thought that transparency would have reduced users' risk perception, since providing more information can possibly mitigate users concerns. Instead, experimental data shows an opposite trend. This trend is particularly evident in the kiosk condition, although still not statistically significant. In addition, current privacy legislation is not considering the impact that the physical design of the system can have on users' privacy considerations. Nevertheless, we have demonstrated that the physical design of the system does significantly affect users' privacy concerns: the embodied design of a humanoid robot is able to mitigate users concerns and collect more private information compared to a dis-embodied system.

Given these findings, we think that present privacy legislation may allow misleading usage of technologies. For example, businesses using technologies to provide services to users may adhere to privacy legislation by disclosing all the necessary information required by law and providing the necessary rights to users. However, they can decide to use a robot with a particular physical design and to develop specific robot's behaviours with the aim to reduce users' privacy concerns. This would allow them to collect much more users' private data compared to other types of technologies, or even robots. Therefore, we recommend that privacy legislation should take into account aspects related to the physical design of the technology and how the designed interactions of the technology may interact with users' privacy considerations.

7 CONCLUSIONS, LIMITATIONS AND FUTURE WORK

In this paper we investigated the effects of transparency on users' privacy considerations and user experience. We predicted that providing to users a reference to the considered privacy policies and additional information on how their data is processed, stored, used and shared would: (H1) increase users' risk tolerance, decrease users' privacy concerns and significantly increase the amount of collected private information; and that (H2) provide a better understanding of the system and therefore a significantly more positive user experience. Indeed, we were able to validate our second hypothesis (H2), namely that transparent information can lead to a better user experience as compared to not providing transparent information. However, we did not find enough evidence to support our first hypothesis (H1).

The present study does not come without some limitations. Firstly, the number of participants in each group was not high. This might have reduced the effect size and prevented significant effects between groups. Secondly, our findings are currently limited to the present context of study, namely a face enrolment system situated in a bank environment. Different applications, framing contexts and types of technologies may determine different effects.

Our future works include the investigation of personality traits possibly involved in decisions concerning users' privacy, the design of a new experiment sharing a similar methodology but involving a different commercial application to investigate if the detected effects are more general, and the study of persuasion in privacy research. We also aim to compare different types of commercial robot platform within a similar methodology. These studies will benefit privacy and user experience research, especially in the field of human-robot interactions and social robotics.

ACKNOWLEDGMENTS

This research is supported by an Australian Government Research Training Program Scholarship and the CBA-UTS Social Robotics Partnership.

REFERENCES

[1] Brandon Amos, Bartosz Ludwiczuk, and Mahadev Satyanarayanan. 2016. *OpenFace: A general-purpose face recognition library with mobile applications*. Technical Report. CMU-CS-16-118, CMU School of Computer Science.

[2] Pauline Anthonysamy, Phil Greenwood, and Awais Rashid. 2013. Social networking privacy: Understanding the disconnect from policy to controls. *Computer* 46, 6 (2013), 60–67.

[3] Iqra Basharat, Farooque Azam, and Abdul Wahab Muzaffar. 2012. Database security and encryption: A survey study. *International Journal of Computer Applications* 47, 12 (2012), 28–34.

[4] Mary J Culnan and Sandra Milberg. 1998. The second exchange: Managing customer information in marketing relationships. (July 1998). https://dx.doi.org/10.2139/ssrn.2621796.

[5] Tamara Dinev and Paul Hart. 2006. An extended privacy calculus model for e-commerce transactions. *Information Systems Research* 17, 1 (2006), 61–80.

[6] Benjamin Fung, Ke Wang, Rui Chen, and Philip S Yu. 2010. Privacy-preserving data publishing: A survey of recent developments. *ACM Computing Surveys (CSUR)* 42, 4 (2010), 14.

[7] James V Haxby, Elizabeth A Hoffman, and M Ida Gobbini. 2002. Human neural systems for face recognition and social communication. *Biological psychiatry* 51, 1 (2002), 59–67.

[8] Stephen Hinde. 1998. Privacy and security—The drivers for growth of E-Commerce. *Computers & Security* 17, 6 (1998), 475–478.
[9] Takayuki Kanda, Masahiro Shiomi, Zenta Miyashita, Hiroshi Ishiguro, and Norihiro Hagita. 2010. A communication robot in a shopping mall. *IEEE Transactions on Robotics* 26, 5 (2010), 897–913.
[10] Taemie Kim and Pamela Hinds. 2006. Who should I blame? Effects of autonomy and transparency on attributions in human-robot interaction. In *The 15th International Symposium on Robot and Human Interactive Communication, 2006.* IEEE, 80–85.
[11] Joseph A Konstan and John Riedl. 2012. Recommender systems: from algorithms to user experience. *User Modeling and User-Adapted Interaction* 22, 1 (2012), 101–123.
[12] Kat Krol, Jonathan M Spring, Simon Parkin, and M Angela Sasse. 2016. Towards robust experimental design for user studies in security and privacy. In *The 4th LASER Workshop (2016): Learning from Authoritative Security Experiment Results.* IEEE, 21–31.
[13] Marc Langheinrich. 2001. Privacy by design—principles of privacy-aware ubiquitous systems. In *Ubicomp 2001: Ubiquitous Computing*. Springer International Publishing, 273–291.
[14] Robert S Laufer and Maxine Wolfe. 1977. Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues* 33, 3 (1977), 22–42.
[15] Bettina Laugwitz, Theo Held, and Martin Schrepp. 2008. Construction and evaluation of a user experience questionnaire. In *Symposium of the Austrian HCI and Usability Engineering Group*. Springer International Publishing, 63–76.
[16] Illah R Nourbakhsh, Clayton Kunz, and Thomas Willeke. 2003. The mobot museum robot installations: A five year experiment. In *Proceedings of IEEE/RSJ International Conference on Intelligent Robots and Systems, 2003 (IROS 2003)*, Vol. 4. IEEE, 3636–3641.
[17] Yves Poullet. 2010. About the E-Privacy Directive: towards a third generation of data protection legislation? In *Data protection in a profiled world*. Springer International Publishing, 3–30.
[18] Anna Romanou. 2017. The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise. *Computer Law & Security Review* (2017), 1–12. https://doi.org/10.1016/j.clsr.2017.05.021
[19] Matthew Rueben, William D Smart, Cindy M Grimm, and Maya Cakmak. 2017. Privacy-Sensitive Robotics. In *Proceedings of the Companion of the 2017 ACM/IEEE International Conference on Human-Robot Interaction*. ACM, 425–426.
[20] Trenton Schulz and Jo Herstad. 2017. Walking Away from the Robot: Negotiating Privacy with a Robot. In *Proceedings of British HCI Conference*. BISL, 1–6.
[21] Rashmi Sinha and Kirsten Swearingen. 2002. The role of transparency in recommender systems. In *CHI'02 extended abstracts on human factors in computing systems*. ACM, 830–831.
[22] Dag Sverre Syrdal, Michael L Walters, Nuno Otero, Kheng Lee Koay, and Kerstin Dautenhahn. 2007. He knows when you are sleeping-privacy and the personal robot companion. In *Proceedings of Workshop on Human Implications of Human–Robot Interaction*. AAAI, 28–33.
[23] The European Parliament and the Council of the European Union. 2016. Directive 95/46/EC (General Data Protection Regulation). (2016). http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679
[24] Meg Tonkin, Jonathan Vitale, Sarita Herse, Mary-Anne Williams, William Judge, and Xun Wang. 2018. A Design Methodology for the UX of HRI: Example Study of a Commercial Social Robot at an Airport. In *Proceedings of ACM/IEEE International Conference on Human-Robot Interaction (HRI2018), Chicago, Illinois USA, March 2018*. ACM.
[25] Meg Tonkin, Jonathan Vitale, Suman Ojha, Jesse Clark, Sammy Pfeiffer, William Judge, Xun Wang, and Mary-Anne Williams. 2017. Embodiment, Privacy and Social Robots: May I Remember You?. In *Proceedings of the 9th International Conference on Social Robotics (ICSR 2017), Tsukuba, Japan, November 22-24, 2017*. Springer International Publishing, Cham, 506–515. https://doi.org/10.1007/978-3-319-70022-9_50
[26] Meg Tonkin, Jonathan Vitale, Suman Ojha, Mary-Anne Williams, Paul Fuller, William Judge, and Wang Xun. 2017. 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, 42–49. https://doi.org/10.1109/ROMAN.2017.8172278
[27] Carl W Turner, Merrill Zavod, and William Yurcik. 2001. Factors that affect the perception of security and privacy of ecommerce web sites. In *Fourth International Conference on Electronic Commerce Research, Dallas TX*. Citeseer, 628–636.
[28] Jonathan Vitale, Meg Tonkin, Xun Wang, Suman Ojha, Mary-Anne Williams, and William Judge. 2017. 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, 439–442.
[29] Mary-Anne Williams. 2009. Privacy management, the law & business strategies: A case for privacy driven design. In *International Conference on Computational Science and Engineering, 2009*, Vol. 3. IEEE, 60–67.
[30] Robert H Wortham and Andreas Theodorou. 2017. Robot transparency, trust and utility. *Connection Science* 29, 3 (2017), 242–248.
[31] Kuang-Wen Wu, Shaio Yan Huang, David C Yen, and Irina Popova. 2012. The effect of online privacy policy on consumer privacy concern and trust. *Computers in human behavior* 28, 3 (2012), 889–897.