Classification of personal data used by personalised robot companions based on concern of exposure

Lewis Riches[1 [0000−0001−9606−820X]], Kheng Lee Koay[1 [0000−0002−5930−6421]], and Patrick Holthaus[1 [0000−0001−8450−9362]]

Adaptive Systems Research Group, University of Hertfordshire,
College Lane, Hatfield, AL10 9AB, UK.
l.riches@herts.ac.uk, k.l.koay@herts.ac.uk, p.holthaus@herts.ac.uk

Abstract. We present a paper looking at the accidental exposure of personal data by personalised companion robots in human-robot interaction. Due to the need for personal data, personalisation brings inherent risk of accidental personal data exposure through multi-modal communication. An online questionnaire was conducted to collect perceptions on the level of concern of personal data being exposed. The personal data examined in this paper has been used to personalise a companion robot along with links to the UK general data protection act. The level of concern for these personal data has been classified into high, medium, and low concern with guidelines provided on how these different classifications should be handled by a robot. Evidence has also been found that age, gender, extroversion, and conscientiousness influence a person's perceptions on personal data exposure concern.

Keywords: Human-Robot Interaction · Companion robots · Personalisation · Personal data security · General Data Protection Regulation

1 Introduction

Companion robots have been defined as specifically designed robots for personal use in the home [3], this key aspect of bringing robots into the home has led a push towards making them personalised within human-robot interaction (HRI). Personalising companion robots allows the systems to use personal data to adapt their functions/actions to be specific to the user. Examples within literature include, a personalised healthcare assistant robot requiring user health data such as a current medication list to enable medication reminders, a personalised bartender robot [17] requiring personality traits and personal preferences to provide personalised communication and drink recommendations and, a personalised robot tutor [9] requiring an initial skill assessment (educational activities) before being able to apply personalised lessons.

As shown a key requirement of personalisation is personal data, without the personal data of the user, the robot is not able to personalise its actions or functions. Personal data has been defined under UK law by the UK general data

protection regulation (UK GDPR) as "any information relating to an identified or identifiable natural person". The requirement of personalisation to need personal data is a potentially limiting factor for the adoption and use of personalised features within robots, due to data privacy and security concerns by the user. Lutz et al. [11] identified the potential of a privacy paradox within personalised robots, showing users wanting personalised actions but being unwilling to provide personal data to a robot due to data security concerns. Denning et al. [4] and Krupp et al. [7] demonstrate the potential security vulnerabilities current commercially available companion robots have such as being stolen/hacked or personal information stored being accessed by someone external. Butler et al. [2] identified data privacy concerns related to a robots ability to capture visual data that could contain sensitive information for example bank cards. Syrdal et al. [20] identified privacy concerns with sharing personal data with a robot companion such as concerns of the robot sharing the personal data with a third party and data on the robot being hacked or stolen.

A key theme through robot data privacy concern literature, is the concern of personal data being stolen or obtained by unauthorised people. For personalised robots to overcome these concerns they need to develop a state of trust with the human they interact with, otherwise the robots personalised features/functions will not be used due to the user not trusting the robot with their personal data. Martin et al. [13] found a relationship between trust and data privacy, identifying that even a small data breach has negative effects on trust. With the goal of promoting trust in HRI so humans use personalised behaviours, personalised robots need to demonstrate data privacy features, with Richards [15] identifying data privacy behaviour as a key in enabling trust. Current solutions deployed in human-computer interaction (HCI) to promote trust in personal data storage such as, the encryption of stored personal data or double authentication can be used in HRI but cannot be the sole data protection method. The provided HCI solutions protected the personal information while being stored on the robot, but companion robots within HRI need to decide when personal information can be exposed, for example not saying personal data in-front of strangers in the home such as a plumber when the robot communicates with its user.

An initial step in teaching robots when personal data can be exposed is for these systems to understand the social contexts personal data is allowed to be shared in to prevent accidental exposure of personal data as identified by Marchang and Di Nuovo [12]. They provide a blockchain authentication method as a potential solution to this challenge, the use of a blockchain approach increases the transparency of personal data being stored and worked on within the robot while also providing the security of blockchain. However, blockchain requires the user to define levels of sensitivity/security of personal data in order to operate, this is an issue as with the varying and large quantity of personal data within HRI, this could be a tedious task in identifying the sensitivity of each personal data or be inaccurate when grouping them. A potential solution to this issue is by using a contextual integrity framework as identified by Rueben et al. [18]. Contextual integrity [14] states that a data breach has occurred when

the norm of appropriateness or distribution have been broken within a given social context, within HRI this would enable a robot to understand when it can share personal data within a social context and not cause a personal data breach autonomously.

The first step in implementing a contextual integrity framework or something similar, is having robots understand how concerning personal data is if it is exposed. These systems will make the decisions of when personal data can be exposed which requires the robot to judge how concerning the personal data would be if it was exposed in that given context. For example, Rossi et al. [16] investigated a Customers' perceived sensitivity of information shared with a robot bartender. However, before a robot can make decisions based on the social context influences, its first needs to understand generally how concerning that personal data is if exposed in a generalised context. UK law provides some classification of the potential concern of personal data exposure by classifying some personal data into a special category [21] meaning we would consider this as high concern personal data. However, the range of personal data this law covers is limited, for example this law does not cover personal preferences which were used by personalised bar tending robot [17] or educational activities used by a personalised robot tutor [9].

This paper will investigate human perception on how concerning personal data is if it was available to the general public to derive a context independent classification. The personal data analysed within this study has all been used or could be used to personalise companion robots within HRI. Individual differences such as personality type, age and gender all influence how we behave as a person and make us unique, within HCI Li et al. [10] has shown a link between a user's personality traits and their views on data privacy sensitivity. Due to these factors this paper will also be investigating if individual differences such as personality types, age or gender influence a persons' judgement on how concerning personal data is when exposed to the general public. This paper aims to answer the following research questions: research question 1 (**RQ1**) can personal data used by a companion robot for personalised assistance be classified based on the concern of exposure?, and research question 2 (**RQ2**) can individual differences influence a person's views on how concerning personal data is if exposed to the general public?. For that purpose, we present the design and conduction of an online questionnaire in Sect. 2, analyse the obtained results in Sect. 3 and discuss implications of our findings to how our classification could be used within HRI in Sect. 4 before concluding the paper in Sect. 5.

2 Methodology

To investigate the research questions listed previously, we conducted an online questionnaire ethically approved by the Health, Science, Engineering and Technology ECDA committee (SPECS/PGR/UH/04859), with recruitment being done through social media and personal social networks. Participants voluntarily filled in the questionnaire with no compensation given for filling it in.

To maintain the aim of a context independent classification of personal data exposure concern, the questionnaire was designed to not include the word robot or any information on the social context.

2.1 Participants details

The first section of the questionnaire was used to collect information about the participant which was: age, gender, and personality trait. This information was collected to enable analysis for **RQ2** and was collected anonymously by not collecting email addresses or names. To collect personality traits the ten item personality measure (TIPI) [6] was used to measure the big five dimensions (Extraversion, Agreeableness, Conscientiousness, Emotional Stability, Openness to Experiences). Along with being a concise scale, TIPI has been shown to provide a strong validity [1], allowing for an accurate representation of a participants personality types, which will then be used to understand the influence personality types have on personal data sensitivity **RQ2**. A text box was used to allow participants to type their gender identity.

2.2 Personal Data

While this paper could not analyse every piece of personal information, thirteen pieces of personal information were chosen due to their link with UK law, use within literature of robot personalisation or use case to enable personalisation for companion robots within HRI (shown in Table 1). Four pieces of personal information come from the special category of UK GDPR [21] that provide information on the user (Health records used by personalised healthcare robots [5], Political opinions, Racial or Ethnic origin and Sexual orientation). Five pieces of personal information pertain to a user's personal preferences (Drink preferences, Food preferences, Movie preferences, Music preferences and Sports preferences) that have been used to personalise a bartending robot when suggesting drinks or topics of conversation [17], and four pieces of personal information have applications to be used for personalisation and use within smart assistant (Calendar appointments, Educational activities used by a personalised tutor robot [9], Employment history, and Financial records).

2.3 General views on personal data sensitivity

Once participants answered the initial questions, each participant was presented with the same following question "For each item select how you would feel if the following information about you were available to the general public.", with participants rating the thirteen individual items of personal data shown in Sect. 2.2, using a 5-point Likert scale (1=Not at all concerned, 2=Slightly concerned, 3=Somewhat concerned, 4=Moderately concerned and 5=Extremely concerned).

2.4 Participants

A total of 102 participants were recruited with 51 being male and 51 being female, with no participants identifying as another gender. The lowest age of the sample was 19 and the maximum age within the sample was 83 with an interquartile range between 23 years old and 40 years old.

2.5 Statistical methods

Research question 1 (**RQ1**) aims to provide the classification of concern of personal data being exposed, to achieve this classification factor analysis will be used. Factor analysis is a reduction technique and reduces a large quantity of variables into factors, this technique will be leveraged to provide evidence of why we classify individual personal data (variables) into concern levels (factors).

Research question 2 (**RQ2**) aims to examine the groups within our sample to see if gender, age and personality type have an influence on the concern level identified in **RQ1**. The Shapiro-Wilk test is used to test for normality over a given data set, for this paper this test showed that the dependent variables were not normally distributed meaning only non-parametric tests could be used. To ascertain if there was a statistical difference between participants within a group, gender and personality types were split into binary groups and age was split by generation [19] (Silent, Boomer, Gen X, Gen Y, Gen Z). For binary groups the Mann-Whitney U test was used and for age the Kruskal-Wallis H test was used to see if there were statistical differences between these groups, to measure correlation Kendall's Tau-b was used.

3 Results

3.1 Classification of personal data

To classify the results based on the concern of exposure factor analysis was performed across all 13 pieces of personal information. A Kaiser-Meyer-Olkin Measure of Sampling Adequacy (KMO=.878) and Bartlett's Test of Sphericity ($X_2(78)$=1058.843, p<.001) indicate the results obtained are fit for this analysis. Factor analysis indicated three factors (Table 1): (1) Low concern, (2) Medium concern, and (3) High concern. Figure 1 shows a bar chart breakdown of the frequencies within these three factors. Racial or Ethnic Origin which has a median of Not at all Concerned, which coincides with the medians in the Low Concern group has been classified as medium concern by factor analysis showing the median cannot be solely relied on for classifying personal data exposure concern. All personal preferences we grouped into the Low Concern category, Medium concern contains three of the four personal information located in the special category of UK GDPR (Political opinions, Sexual orientation and Racial or ethnic origin) along with educational activities and employment history, and High concern has Financial records, Health records and Calendar appointments.

Table 1. Results of Factorial Analysis identifying three components across the thirteen items of personal information, personal information marked with a ∗ is personal information within the special category of UK GDPR

Personal information	Components		
	1	2	3
Music interests	0.905		
Sport preferences	0.879		
Interest in movies	0.841		
Drink preferences	0.839		
Food preferences	0.831		
Political opinions∗		0.812	
Sexual orientation∗		0.71	
Educational activities		0.661	
Racial or ethnic origin∗		0.62	
Employment history		0.595	
Financial records			0.92
Health records∗			0.897
Calendar appointments			0.807

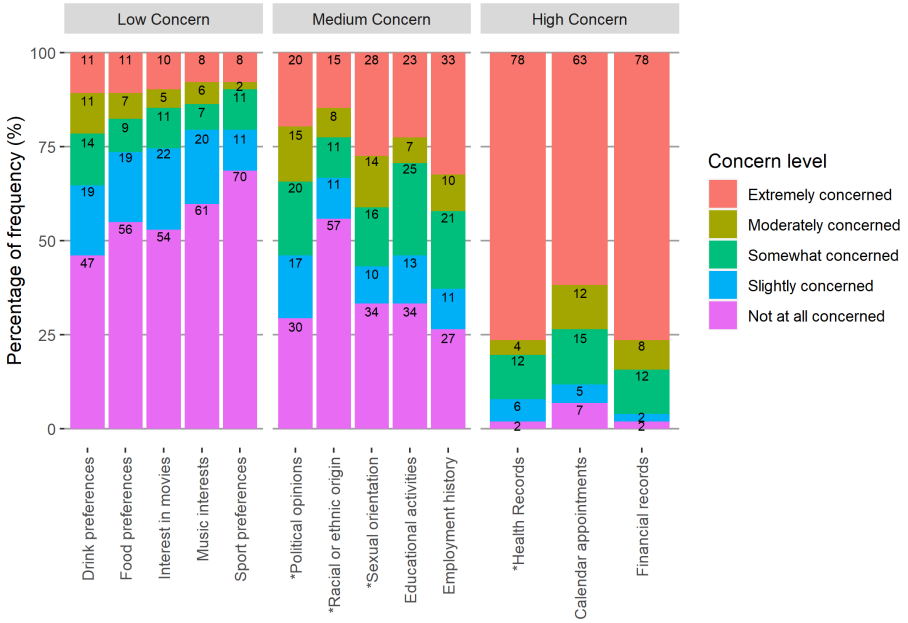

Fig. 1. Participants perceptions on the concern level of each individual item of personal data being available to the general public grouped into components identified in factorial analysis, with X axis being each individual item of personal data, Y axis being the percentage of participants (total participants is 102) and labels on the bar being the frequencies for each bar, personal information marked with a ∗ is personal information within the special category of UK GDPR

3.2 Influencing factors on personal data sensitivity

Mann-Whitney U tests were conducted across age, gender, and personality types using these as the independent variables and the individual items of personal data as the dependent variable. Statistical significance was only found for age, gender, extroversion, and conscientiousness.

Gender for this paper is considered a binary variable as shown in Set. 2.4, in our sample 51 participants identified themselves as male and 51 participants identified themselves as female. Results from the Mann-Whitney U tests found gender to be statistically significant only for Sports preferences (U=973, p=.008, r=.264) with males having a lower concern rank compared to females. While only sports preference was found to have statistical significance a clear pattern was identified in the Kendall-Tau B correlation showing that for each individual item of personal data males ranked concern lower than females.

Age was considered to not be binary and initially have 5 groups dictated by generations with the following frequencies N_{Silent}=1, N_{Boomer}=2, N_{GenX}=18, N_{GenY}=43, N_{GenZ}=38. Both the Silent and Boomer generations had frequencies of 1 and 2 so for our analysis these were removed meaning we only used responses from participants who are in generations X, Y and Z totalling 99 responses. Results from the Kruskal-Wallis H test found age to be statistically significant for Health records (X_2=6.686, p=0.035), Political opinions (X_2=9.275, p=0.01), Sexual orientation (X_2=9.097, p=0.011), Drink preferences (X_2=6.937, p=0.031), Music Preferences(X_2=8.412, p=0.015), Educational activities (X_2= 7.543, p=0.023), and Calendar appointments (X_2=11.112, p=0.004). In all cases the Kendall-Tau B correlation showed a positive correlation meaning that as age increases, the concern rank also increases.

The TIPI scale outputs a score of low, medium low, medium high or high ranking for the five personality dimensions (Extroversion, Agreeableness, Conscientiousness, Emotional Stability, Openness to Experiences) [6]. Each dimension was split into 2 groups: Low which contained outputs low and medium low, and High which contained outputs medium high and high. Of the five dimensions only extroversion and conscientiousness were found to have any statistical significance. **Extroversion** had frequencies of 51 for the Low group (G1) and 52 for the High group (G2) and was found to be statistically significant for: Political opinions (U=919, p=0.01, r=0.26, T_B=-0.23), Sexual orientation (U=928, p=0.01, r=0.25, T_B=-0.23), Racial or ethnic origin (U=850, p=<.001, r=0.33, T_B=-0.31), Movie preferences (U=908, p=0, r=0.28, T_B=-0.26), Sport preferences (U=1020.5, p=0.02, r=0.23, T_B=-0.22), and Music preferences(U=922, p=0, r=0.28, T_B=-0.27). A negative correlation was found for all statistically significant results indicating as a participant became more extroverted, their concern ranking decreased. **Conscientiousness** with frequencies of 46 for the Low group (G1) and 56 for the High group (G2), was found to be statistically significant for : Political opinions (U=943, p=0.02, r=0.24, T_B=0.21), Racial or ethnic origin (U=1008.5, p=0.04, r=0.21, T_B=0.19), Drink preferences (U=923, p=0.01, r=0.26, T_B=0.24), and Sport preferences (U=1045.5, p=0.05, r=0.2,

T_B=0.19). The Kendall-Tau B correlation for these results was positive, showing as conscientiousness increases, a person's concern ranking also increases.

4 Discussion

The classification outset in Sect. 3.1 provides the first step in being able to train personalised companion robots on how sensitive personal data is (RQ1), enabling such a system to not accidentally expose sensitive personal data while communicating with a user. For example, personal data classified as High concern by default is never exposed and HCI methods such as sending the information via a mobile notification or asking for further verification (e.g. facial or voice recognition) before communicating the personal data, and personal data classified as Low Concern is freely exposed without any restrictions. However, personal data classified as Medium Concern is not as straightforward, this is due to the polarised nature of this information within the classification as shown by the frequencies in Fig. 1. This paper suggests a user input approach for such a classification where a user decides how this personal data should be handled and robots' default to High Concern processes until specified otherwise.

Shown in Sect. 1 to enable personalised behaviours for robots within HRI a user needs to trust the robot with their personal data. Both Richards [15] and Martin et al. [13] shows that trust is promoted by data protection behaviour, meaning if robots exhibit data protection behaviour using our classification as shown above, this will promote user trust of the robot enabling the further sharing of personal data and further personalised behaviour being used. Transparency has been shown to allow users to understand the actions of the robot better [8] and also regain trust quicker if an error does occur transparency. A reason-based approach to personal data communication using our classification, for example, if a robot sends the personal data via a phone notification, will enable transparency for the user as they will know it has been communicated in this way as the personal data is classified as High Concern.

This classification not only provides guidelines for how robots should handle personal data but also for HRI researchers and people actively working in the field of companion robotics/personalised robotics. For example, instead of collecting Health records (High Concern personal data) to assess participants' food allergies, ask only for food preferences (Low Concern personal data). Using less sensitive data within studies to obtain the same result, may make participants feel more comfortable providing such data within the studies, along with potentially improving data collection practices within HRI.

Of particular interest with our classification is the classification received for the personal data derived from the special category data in the UK GDPR [21]. Due to this personal data being derived from law, it could be inferred that this personal data would be classified as High Concern. However, the classification provided shows only one of the four individual items of personal data (Health records) being classified as High Concern with the remaining three being classified as a Medium Concern. A causal factor for this could be due to the person's

understanding of what is protected under UK law. For HRI this means robots could provide users with informed consent on local law to make sure they are aware of how their personal data is protected under local law. The classification presented in this paper does not supersede the local law of how personal data should be handled. For example, while only one of the four personal data from the special category data in the UK GDPR was classified as High Concern, all four should be considered high concern and follow the further rules set out by the UK GDPR, then allow users to change this classification manually if they choose to do so.

These results show age, gender, extroversion, and conscientiousness as paramount influencing factors on how participants perceive personal data exposure concerns (**RQ2**). These results are in partial agreement with Li et al. [10] who identified a similar influencing factor within HCI of extroversion, however, this paper found no link between openness and a participant's views on personal data exposure concerns. This paper argues based on the identification of these influencing factors, that not only does the concern classification personal data is in need to be considered but also the age, gender, extroversion, and conscientiousness of the person whose personal data is being communicated needs to be considered. Future work could investigate a combinational effect of both the context and influencing factors may have on personal data exposure concern.

Section 1 identifies the potentiality of using a contextual integrity framework within HRI as a solution to prevent the accidental exposure of personal data by a personalised robot within HRI. Using this classification and the factors that can influence this, robots can start to be trained to understand how sensitive personal data is, working towards the norm of appropriateness/disruption aspects of contextual integrity [14]. This classification also provides motivation for the need of such frameworks within HRI due to different contexts influencing the sensitivity of personal data. Work from Rossi et al. [16] looked at personal data sensitivity within a public bar context and found increased concern rankings for: all personal data that overlapped with this work (Rossi et al. mean (M_R, this papers mean M_L) : political opinions (M_R =4.09, M_L=2.78), sexual orientation (M_R=3.84, M_L=2.92), movie preferences (M_R=2.49, M_L=1.97), drinks preference (M_R=2.34, M_L=2.22), and sports preferences (M_R=2.34, M_L=1.70).

5 Conclusion

This paper has provided a classification of personal data as a solution to concerns of personal data being accidentally exposed within HRI, with a classification of low, medium and high concern. This paper has identified guidelines on how this classification can be used within both robot design and HRI study design. Influencing factors on this classification have been identified as age, extroversion and conscientiousness which need to be factored into a policy derived from these classifications. Care needs to be taken with using any personal data within HRI and all guidance from the local law needs to be considered before this classification is applied.

References

1. Ahmed, A.O., Jenkins, B.: Critical synthesis package: Ten-item personality inventory (TIPI). MedEdPORTAL **9**, 9427 (2013)
2. Butler, D.J., Huang, J., Roesner, F., Cakmak, M.: Privacy-utility tradeoff for remotely teleoperated robots. pp. 27–34. ACM (2015)
3. Dautenhahn, K., Woods, S., Kaouri, C., Walters, M., Koay, K., Werry, I.: What is a robot companion - friend, assistant or butler? pp. 1192 – 1197 (09 2005)
4. Denning, T., Matuszek, C., Koscher, K., Smith, J.R., Kohno, T.: A spotlight on security and privacy risks with future household robots. pp. 105–114. ACM (2009)
5. Fiorini, L., Esposito, R., Bonaccorsi, M., Petrazzuolo, C., Saponara, F., Giannantonio, R., Petris, G.D., Dario, P., Cavallo, F.: Enabling personalised medical support for chronic disease management through a hybrid robot-cloud approach. Autonomous Robots **41**, 1263–1276 (2017)
6. Gosling, S.D., Rentfrow, P.J., Swann, W.B.: A very brief measure of the big-five personality domains. Research in Personality **37**, 504–528 (2003)
7. Krupp, M.M., Rueben, M., Grimm, C.M., Smart, W.D.: A focus group study of privacy concerns about telepresence robots. pp. 1451–1458. IEEE (2017)
8. Kulesza, T., Stumpf, S., Burnett, M., Yang, S., Kwan, I., Wong, W.K.: Too much, too little, or just right? ways explanations impact end users' mental models. In: 2013 IEEE Symposium on VL/HCC. pp. 3–10 (2013)
9. Leyzberg, D., Spaulding, S., Scassellati, B.: Personalizing robot tutors to individuals' learning differences. pp. 423–430. ACM (2014)
10. Li, Y., Huang, Z., Wu, Y.J., Wang, Z.: Exploring how personality affects privacy control behavior on social networking sites. Frontiers in Psychology **10** (2019)
11. Lutz, C., Tamó-Larrieux, A.: The robot privacy paradox. Human-Machine Communication **1**, 87–111 (2020)
12. Marchang, J., Di Nuovo, A.: Assistive multimodal robotic system: Security and privacy issues, challenges, and possible solutions. Applied Sciences **12**, 2174 (2022)
13. Martin, K.D., Borah, A., Palmatier, R.W.: Data privacy: Effects on customer and firm performance. Journal of Marketing **81**, 36–58 (2017)
14. Nissenbaum, H.: Privacy as contextual integrity. Wash. L. Rev. **79**, 119 (2004)
15. Richards, N.M., Hartzog, W.: Taking trust seriously privacy law. SSRN E (2015)
16. Rossi, A., Giulia, P., Silvia, R.: Investigating customers' perceived sensitivity of information shared with a robot bartender. In: Social Robotics. pp. 119–129. Springer International Publishing (2021)
17. Rossi, A., Rossi, S.: Engaged by a bartender robot: Recommendation and personalisation in human-robot interaction. pp. 115–119. ACM (2021)
18. Rueben, M., Aroyo, A.M., Lutz, C., Schmölz, J., Van Cleynenbreugel, P., Corti, A., Agrawal, S., Smart, W.D.: Themes and research directions in privacy-sensitive robotics. In: 2018 IEEE Workshop on Advanced Robotics and its Social Impacts (ARSO). pp. 77–84 (2018)
19. Strauss, W., Howe, N.: Generations: The History of America's Future. Quill (1992)
20. Syrdal, D.S., Walters, M., Otero, N., Koay, K.L., Dautenhahn, K.: "he knows when you are sleeping" - privacy and the personal robot companion pp. 28–33 (2007)
21. United Kingdom Parliment: United kingdom general data protection regulation 2016, no. 679., https://www.legislation.gov.uk/eur/2016/679/contents#