

'He knows when you are sleeping' – Privacy and the personal robot companion

Dag Sverre Syrdal, Michael L. Walters, Nuno Otero, Kheng Lee Koay and Kerstin Dautenhahn

Adaptive Systems Research Group, School of Computer Science, University of Hertfordshire
College Lane, Hatfield,
Hertfordshire, AL10 9AB
{d.s.syrdal, m.l.walters, n.r.otero, k.l.koay, k.dautenhahn}@herts.ac.uk

Abstract

One of the most compelling visions of future robots is that of the robot butler. An entity dedicated to fulfilling your every need. This obviously has its benefits, but there could be a flipside to this vision. To fulfill the needs of its users, it must first be aware of them, and so it could potentially amass a huge amount of personal data regarding its user, data which may or may not be safe from accidental or intentional disclosure to a third party. How may prospective owners of a personal robot feel about the data that might be collected about them? In order to investigate this issue experimentally, we conducted an exploratory study where 12 participants were exposed to an HRI scenario in which disclosure of personal information became an issue. Despite the small sample size interesting results emerged from this study, indicating how future owners of personal robots feel regarding what the robot will know about them, and what safeguards they believe should be in place to protect owners from unwanted disclosure of private information.

Introduction

The work presented in this paper has been carried out as part of the European project Cogniron. The purpose of Cogniron is to study the perceptual, representational and learning capabilities of robots in human centered environments in order to develop methods and technologies for the construction of robots capable of adapting and growing their capacities in close interaction with humans in an open-ended fashion. In the context of the Cogniron project a Robot Companion must fulfill two important functions: a) making itself 'useful', i.e. being able to carry out a variety of tasks in order to assist humans in a domestic home environment, and b) behaving socially, i.e. possessing social skills in order to be able to interact with people in a socially acceptable manner (Syrdal et al., 2006). Finally, such a Robot Companion needs to be adaptive, both in the functions it performs for its users, but also in regard to the social setting in which it performs

these functions, in order to respond to the different needs and preferences of its user.

While research into the development of a robot companion needs to address technical issues related to both of the above functions, we also recognise that such research needs to address the possible wider impact that ownership and use of a personal robot companion will have on future users of this technology. One salient field to address is that of privacy and handling of personal information. The EURON Roboethics Roadmap considers privacy to be one of the ethical problems that has to be addressed in relation to personal robots (Veruggio, 2006). This investigation is an exploratory study, using a human-robot interaction(HRI) scenario, on how potential users of a personal robot companion perceive the possible issues regarding privacy when using a personal robot, and what measures they believe should be in place to best reconcile the need for personal information with the risk of disclosure to third parties.

Privacy

Technological development and dissemination have, in the past, radically and qualitatively altered the way in which, researchers, legislators and the general public think and act regarding issues surrounding privacy and technology. The initial concerns in the 1970s were over a 'Big Brother' state gathering information about its citizens in vast databanks along with those of large corporations, which could be countered almost purely through legislative checks and balanced by governmental institutions set up to regulate the way that these databanks gathered and processed this information. However, the revolution in mini-computing and the advent of smaller, specialized databases at the hand of a wider range of public and commercial organizations made these measures largely redundant, and forced a change both in legislation and public attitudes (Mayer-Schoenberger, 1997). The last 15 years have seen dramatic changes as well, with private use of the internet changing protection of privacy, not only from intrusion by government and commercial interests, but also from

criminal groups; from the responsibility of the state to a matter of personal self defense (Clarke, 1998).

While current information technology like internet use, credit and loyalty cards, and public CCTV networks, all gather information about the individual, this information is restricted to certain arenas of behaviour, such as that in public spaces or economic behaviour. This raises the very real possibility that current concerns and approaches to protection of personal data will change dramatically and qualitatively with a widespread use of autonomous household robots. Exploring the concerns that potential users may have on the issue of privacy, in an open-ended manner, with the aim of obtaining as wide a range of information as possible, is thus integral when considering the impact which this technology will have on the everyday life of its users.

Privacy and the Robot Companion

An adaptive personal robot companion will by its very nature acquire a potentially wide range of information regarding its users and will likely have the capability to gather this information to much larger extent than technology that is currently in private use. A personal robot may need to store information regarding the lay-out of a home and its contents as well as housekeeping styles and preferences of its users, so that it can perform its everyday tasks to the satisfaction of its users. It may also need to store information regarding special needs of its users such as disabilities, illnesses or addictions, in order to compensate for any difficulties a user might have, or to monitor a user's medical condition, or to respond to medical emergencies. In order to perform its tasks in a socially acceptable manner, an adaptive personal robot will also need to be aware of interaction style preferences of its users, both when interacting with a user on a one-on-one basis, but also in social settings with more than one individual present. Information regarding individual differences in comfort-spatial zones may be important for navigation in human-centered settings (Syrdal et al., 2006; Walters et al., 2005). This means that information directly related to the private sphere of the lives of its users is collected, information that is usually not stored or used deliberately by currently existing technology.

The disclosure of information to a third party by a personal robot may be accidental or intentional. Intentional here is taken to mean disclosure of information to a third party that is intended by the designers and/or users of the personal robot. This type of disclosure may be to serve a variety of purposes. A personal robot companion could shop for groceries online, disclosing information regarding credit card accounts to trusted vendors. In assistive robotics robots may monitor and send information to health professionals regarding health-related issues, such as the

use of prescribed medication or rehabilitation progress (Gockley & Matarić, 2006; Takahashi et al., 2002; Tapus & Matarić, 2006). Likewise, manufacturers of robots may wish to access some information regarding user preferences in order to inform the design of future products.

However, there is also the possibility of accidental or unintended information disclosure to a third party. One issue here is that of security. Probably a personal robot may be in communication with a computer network, belonging to its users, which may be connected to the internet, and as such existing issues with personal security related to intrusion, viruses, and other malware may be applicable to personal robots. It is also not inconceivable that malware that specifically targets personal robots may be developed in order to obtain information of a private nature from personal robots. Also, a personal robot may give information out to a third party through a fault in its programming and/or behaviour.

Accidental information disclosure may also happen implicitly, through a personal robot's behaviour in the presence of a third party. As both the tasks that the robot performs for its users as well as its social behaviour should be adapted for each individual user, the manner in which it interacts with its user could give a third-party observer information regarding individual preferences. As appropriate social behaviour for a robot interacting with humans has been shown to be related to the personality of the user (Gockley & Matarić, 2006; Syrdal et al., in Press; Syrdal et al., 2006; Walters et al., 2005), observation of such interactions may reveal information about the user's personality traits.

Towards this Study

In conclusion, it seems that a personal robot companion can potentially be perceived as a 'walking CCTV camera' that continuously stores information about its environment and those within, as well as having the capability of autonomously revealing this information to third-parties. In light of this, studying the attitudes and opinions possible users of such technology may develop towards this technology, is important, not only for developing systems to prevent unauthorized access to information, but also in order to investigate to what extent future users will allow and tolerate the intrusion of personal robots on different aspects of their personal lives.

Method:

Apparatus:

The robot used for this particular study was a PeopleBot™ (commercially available from ActivMedia Robotics). The

PeopleBot is human-sized and mechanical in appearance. In this study the robot was operated under remote control, a method known as the Wizard of Oz Method (Walters et al., 2005).

Participants:

Due to the nature of the study, the participants were drawn from a long-term study that investigated several human-robot interaction issues including social spaces and approach distances, and using different social interaction scenarios. The sample contained students and staff based at University of Hertfordshire, from various disciplines including computer science, psychology, physics, mathematics, business studies and marketing. As this sample was drawn from a cross-section of a British student/staff population it contained participants from British, Greek, Indian, Pakistani and Indonesian nationalities.. Prior to the trial on privacy issues the participants had been exposed to the robot as part of their participation in our long-term study. The group of participants as such represented a non-expert sample which would be proficient in exploring possibly issues emerging from the use of personal robot companions.

Procedure:

As the technology required to create long-term robot companions capable of storing information about its users is not readily available, the experiment was scenario-based. The use of scenarios to investigate the possible impact of new technologies has been used extensively, albeit mostly within an occupational setting (Carroll, 1996; Rosson & Carroll, 2001). However, studies have aimed at introducing scenarios within home settings as well as within pastiches of fictional scenarios in order to allow potential users of emerging technology a more informed understanding of its possible impact (Blythe & Wright, 2006; Newell et al., 2006). The present investigation decided to simulate the scenario of a conversation between two people about personal habits. This is a common scenario, and most people tend to engage in this type of conversation on a regular basis with new acquaintances. As such we expected that all the participants were familiar with the scenario.

The scenario was performed in the University of Hertfordshire Robot House, a privately rented flat which is used for HRI experiments, in order to increase the ecological validity of the setting. Individual participants were seated on a sofa with the experimenter and told that they were going to have a conversation. A Peoplebot was also present during the conversation, trying to "behave socially" and join in the conversation. The experimenter would guide the conversation through asking the participants about their opinions on various topics, ranging from sleeping and housekeeping habits, to attitudes towards healthy eating and smoking. The experimenter

would also disclose personal information to the participants. At predetermined points in the conversation, the Peoplebot would interrupt the experimenter in order to volunteer factually correct, yet socially inappropriate information about the experimenter to the participant. See below for two examples:

Example 1:

Experimenter: "I always try to go to sleep early so I can get a good night sleep."

Robot: "Dag (*the experimenter*) did not go to bed until 3 o'clock last night."

Experimenter: "Well...moving on..."

Example 2:

Experimenter: Do you find enough time to Hoover your apartment every day?

Participant: Some weeks, I find I don't have enough time.

Experimenter: Well, that is one of the handy things about this robot, it can Hoover the house if you load in the right program.

Robot: Dag has not accessed my vacuum-cleaning program for 2 weeks.

After the conversation was finished, the participants were invited to complete a questionnaire and were interviewed by the experimenter.

Measures:

As this was an exploratory study, its main focus was on acquiring as wide a range of responses as possible. As such the questionnaire contained several open-ended questions as well as questions intended to stimulate thought on a variety of issues. The questions are summarised below:

How do you feel about a robot storing information about you? (Likert scale 1-5)

How should a robot treat the information it stores about you and your household?

What category of information are you the *most* comfortable about a robot storing information regarding?

What category of information are you the *least* comfortable about a robot storing information regarding?

The list of categories was as follows, with possible reasons for information storage presented as well.

- Sleeping habits and your daily routine
 - In order to make sure that it doesn't disturb you when it performs its tasks
- Eating and drinking habits

- In order to keep track of food stocks or offer you snacks/drinks when you usually like them
- Housekeeping style
 - In order to tidy and clean in a manner that complements your needs.
- Preferences regarding how the robot should behave in terms of social spaces, dialogue etc.
 - So that the robot can tailor its behaviour according to your likes and dislikes
- Friends and acquaintances
 - In order to accommodate the preferences of your friends when they visit your house, alternatively as a security measure
- Health issues relating to diet and exercise
 - In order to encourage you to do exercise and healthier eating
- Other health issues
 - In order to remind you about medication or particular health risks
- Personality and other psychological characteristics
 - To adapt general aspects of its behaviour to your particular profile
- Demographic information (e.g. Age, Gender, Profession)
 - To adapt general aspects of its behaviour to your particular profile

Results

The responses from the participants were transcribed and later analysed qualitatively by three of the researchers. The findings are reported below:

How do you feel about a robot storing information about you?

Five participants rated their feelings regarding information being stored as Uncomfortable or Very Uncomfortable, 5 participants rated them as Neutral, 2 participants rated them as Comfortable. None rated them as Very Comfortable.

In the reasoning given by the participants for their ratings, two main themes emerged. The first theme, which occurred mainly amongst the participants who stated they were uncomfortable with the robot storing information, was that of the risk of information disclosure (see examples below):

"However, sharing my info with non-friends may not be pleasant"

"Robot could be stolen or hacked into."

"I would be concerned that the robot might reveal personal information of a private nature."

The second theme emerging from this question was that of the utility of storing information, both for the robot when performing its tasks, but also for direct access for the user. This theme appeared mainly amongst participants who described themselves as neutral or comfortable with the robot storing information about them (see below for examples):

"It can somehow understand my likes and dislikes"

"maybe it is useful to review your daily life."

The final theme to emerge for this particular question was a synthesis of the two, where participants described their attitude as the result of a trade-off between the value of the robot storing personal information and the risk of information disclosure:

"I appreciate its usefulness- i.e.- where I left keys etc. but concerned about data protection and security credit card no. etc."

Treatment of Stored information

Two themes emerged from the participants' responses as to how stored information should be treated. The first theme was related to the security measures of the robot and the information stored on it (see examples below):

"Have security codes set up so it's only accessible to the user"

"It would be good if you could trust the robot, if there were safety precautions in place"

The second theme was related to the retention of data. Most of these responses argued for the deletion of data that was not required by the personal robot for carrying out its tasks, or that may be useful for the user of the robot (see below for examples):

"Any irrelevant data should be ignored and deleted from memory"

"Information that it is not appropriate should not be retained for any longer than necessary"

Categories of information:

The most accepted categories of information among the participants were those related to sleep and daily routine; and housekeeping style. The least accepted category was personality and other psychological characteristics. The two health related categories were 'controversial' within

the sample in the sense that 4 participants listed it as the most accepted and 5 listed it as the least accepted.

Studying the participants' reasoning behind being the most comfortable with data on sleep, daily routine and housekeeping, two main themes emerged. The first theme was that participants tended to clearly see the utility of the information being stored and used by the robot, and the second theme was that participants did not see the information as particularly sensitive (examples below):

'The robot can work around my routine without disturbing me.'

'It is the least personal information.'

The main theme for reasoning in not being comfortable regarding the storage of information on personality and other psychological characteristics was that the participants considered this information being more sensitive (see below):

'Because I feel insecure when someone knows my personal details.'

'They are related to a person's self. Not for other people or robots.'

Examining the responses related to the categories involving health issues, we saw two themes emerging. For those participants rating this as the most accepted category, the dominant theme was one of utility:

'Health, diet and exercise, are the things that people forget and never remember.'

'It will help me improve my life to be healthy, particularly relating to medical treatment'

For those participants not comfortable with information regarding these categories being stored the main theme was one of concerns regarding disempowerment, and whether or not it was appropriate for robots be used in this particular sphere of everyday life:

'I should be in charge of my own health'

'Because I would never want to rely on a machine to look after me like that, we should be self-sufficient'

Other issues arising across the questionnaire and interview data:

The first of these themes that arose across the different questions was that of information stored about third parties that are not the primary users of the robot. The two

statements below, given independently by two of the participants are good examples:

'I know it is illegal, but I would be handy to have a stored record of all of my conversations.'

'...I would be concerned around someone else's robot and about the information it collects about me.'

Another issue was the value of the information being stored by the robot for future researchers, both commercial and academic:

'... [The information on the robot] may be useful in the future e.g. medical research. Furthermore my information can be stored and traded to companies.'

A third issue that arose in the semi-structured interviews was that of criminal activities. Most of the participants saw the robot divulging this information to a third party (i.e. the police or other law enforcement agencies) as a problematic issue, both due to a lack of confidence in the robot's ability to identify criminal activities accurately, as well as due to concerns over privacy.

While on the whole, individual differences were more important than cultural differences, one of the differences between cultures was that the participants from Indonesian backgrounds viewed the information stored on the robot as the property and concern of the household as a whole, while participants from other backgrounds were more likely to be concerned about individual data, i.e. individual accounts for each household member, information about one member not being divulged to others etc. This was the only difference we observed related to cultural background.

Discussion and Conclusions

While we do not contend that the responses from this particular sample will be representative of all the concerns that will arise from the use of personal robots, the responses nevertheless raises important issues for researchers and developers in the field of HRI.

The main issue to consider is that none of the participants were completely comfortable with the idea of a personal robot storing information regarding the person or their behaviour, regarding it as a 'necessary evil' that is tolerated as long as there is a clear, perceptible benefit to the user. It is also important to note that, overall, participants' attitudes towards privacy was one of a trade-off between the utility and the how sensitive the nature of

the information was. This suggests that systems that are meant to be used by the general public should strive to explicitly justify any data capture from its users.

Also, the fact that personality and other psychological characteristics are among the categories that participants were the least comfortable with the robot storing information regarding, does raise some ethical questions for researchers who are investigating the role of user personality traits as predictors of HRI preferences. Any direct application of such results could be problematic if the concerns of our sample are shared by the general public.

The results regarding the health categories can be understood to arise from a portion of the sample having misgivings about the use of robots in that particular domain, rather than related to issues of privacy and data protection. As this was not a clinical sample, it is difficult to say if potential users of assistive robotics products would give a similar response.

The wider issues of how the use of personal robots will affect the everyday lives of their users on a number of levels, including that of privacy and data protection, remain an important field of study. The results from our particular exploratory study show that the people who will ultimately decide on the acceptability of a technology, its potential users, offer a rich and interesting source of insight for researchers in the field.

Acknowledgements

The work described in this paper was conducted within the EU Integrated Project COGNIRON ("The Cognitive Robot Companion") and was funded by the European Commission Division FP6-IST Future and Emerging Technologies under Contract FP6-002020.

References

Blythe, M. A.; & Wright, P. C. 2006. Pastiche Scenarios: Fiction as a resource for user centred design. *Interacting With Computers* 18(5): 1139-1164.

Carroll, J. M. 1996. Becoming social: expanding scenario-based approaches in HCI. *Behaviour & Information Technology* 15(4): 266-275.

Clarke, R. 1998. Information Privacy On the Internet - Cyberspace Invades Personal Space. *Telecommunication Journal of Australia* 48(2).

Gockley, R.; & Matarić, M. J. 2006. Encouraging Physical Therapy Compliance with a Hands off Mobile Robot. *Proc. HRI06, Salt Lake City, Utah, USA, 2006*: 150-155.

Mayer-Schoenberger, V. (1997). Generational Development of Data Protection in Europe. In P. E. Agre & M. Rotenberg (Eds.), *Technology and Privacy: The New Landscape* (pp. 219-241). Cambridge, MA: MIT Press.

Newell, A. F.; Carmichael, A.; Morgan, M.; & Dickinson, A. 2006. The use of theatre in requirements gathering and usability studies. *Interacting With Computers* 18(5): 996-1011.

Rosson, M. B.; & Carroll, J. M. 2001. *Usability Engineering: Scenario-Based Development of Human-Computer Interaction*. San Fransisco: Morgan Kaufmann Publishers.

Syrdal, D. S.; Dautenhahn, K.; Woods, S.; Walters, M.; & Koay, K. L. In Press. Looking Good? Appearance Preferences and Robot Personality Inferences at Zero Acquaintance. *Proceedings of 2007 AAAI Spring Symposia*.

Syrdal, D. S.; Dautenhahn, K.; Woods, S.; Walters, M. L.; & Koay, K. L. 2006. 'Doing the right thing wrong' – Personality and tolerance to uncomfortable robot approaches. *Proc. 15th IEEE International Workshop on Robot and Human Interactive Communication (RO-MAN 2006)*: 183-188.

Takahashi, Y.; Goto, H.; & Saito, T. 2002. Health care system using face robot and tele-operation via Internet. *Proceedings of the 7th International Conference on Control, Automation, Robotics and Vision, 2002. ICARCV 2002. 2*: 1025-1030.

Tapus, A.; & Matarić, M. J. 2006. User Personality Matching with Hands-Off Robot for Post-Stroke Rehabilitation Therapy. *Proceedings, 10th International Symposium on Experimental Robotics (ISER-06)*.

Veruggio, G. 2006. EURON Roboethics Roadmap. *EURON Roboethics Atelier, Genoa, 27th of February - 3rd of March 2006*.

Walters, M.; Woods, S.; Koay, K. L.; & Dautenhahn, K. 2005. Practical and methodological challenges in designing and conducting interaction studies with human subjects. *AISB'05 Symposium on Robot Companions Hard Problems and Open Challenges in Human-Robot Interaction*: 110-120.

Walters, M. L.; Dautenhahn, K.; Boekhorst, R. T.; Koay, K. L.; Kaouri, C.; Woods, S., et al. 2005. The influence of subjects' personality traits on personal spatial zones in a human-robot interaction experiment. *Proc. 14th IEEE International Workshop On Robot And Human Interactive Communication (RO-MAN 2005)*: 347-352.