Understanding Users' Perception of Privacy in Human-Robot Interaction

Min Kyung Lee, Karen P. Tang, Jodi Forlizzi, Sara Kiesler
Human-Computer Interaction Institute
Carnegie Mellon University
{mklee, kptang, forlizzi, kiesler}@cs.cmu.edu

ABSTRACT
Previous research has shown that design features that support privacy are essential for new technologies looking to gain widespread adoption. As such, privacy-sensitive design will be important for the adoption of social robots, as they could introduce new types of privacy risks to users. In this paper, we report findings from our preliminary study on users' perceptions and attitudes toward privacy in human-robot interaction, based on interviews that we conducted about a workplace social robot.

Categories and Subject Descriptors
H.m [**Information Systems**]: Miscellaneous

General Terms
Design

Keywords
Privacy, human-robot interaction, social robot, workplace robot

1. INTRODUCTION
Privacy is an individual's right to have control over her own data [5] and is one of the fundamental human rights. Research in human-computer interaction has shown that privacy-sensitive designs that provide users with sufficient levels of awareness and control are critical for the widespread adoption of new technologies [1]. Similarly, designing appropriate privacy features is also important for the successful adoption of social robots. Many social robots are equipped with high-resolution sensors that are capable of collecting large amounts of data about users and environments; this introduces potential privacy risks for those that interact with social robots.

Prior research in HCI has investigated different ways to promote people's privacy in domains like information technology and mobile computing [3]. We, however, posit that designing privacy features for mobile robots requires different treatments from these other fields, based on four observations.

First, as robotic technology advances, the level of interactivity between the robot and user has led to an increasingly sophisticated array of sensors that is more extensive than what is normally seen on devices such as mobile phones. The complexity of such sensing can lead users to underestimate the capabilities of the robot and misunderstand how and what kinds of data are being recorded.

Second, the mobility and autonomy of robots can often blur the traditional boundaries between private and public spaces. For example, video surveillance is, more or less, acceptable in public spaces, but not in private places. In addition, it is still unclear what rules should be adaptively applied to robots that navigate in both public and private places (e.g., robots that operate in a hospital or in an office environment).

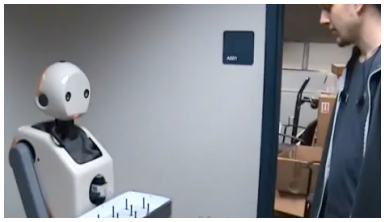

Figure 1. A screenshot of the video scenario where the Snackbot is interacting with a user in a hallway of an office building.

Third, many social robots use human-like conversational language to interact with users and are often anthropomorphized by users. Through these interactions, trust and attachment may form between users and robots, which, in turn, could be used to influence (or even manipulate) users to spontaneously disclose private or sensitive information to robots. This interaction pattern is distinct from how users commonly interface with devices like the mobile phone.

Finally, because of its high operating costs, many social robots, such as those found at workplaces, tend to be shared between several users. These robots often only have a single interface for viewing and collecting data, which could make one's data more easily accessible by others. In addition, as robots often share a physical space with other people, robots could accidently collect data from by-standers while they engage with their primary users.

To explore ways of designing privacy-sensitive features, we first sought to understand users' perceptions of privacy with social robots. Specifically, we focused on assessing (i) how well users understand the types of data that robots collect, and (ii) their attitudes toward such data collection (including cases of accidental data collection, e.g., from by-standers).

2. METHOD
We conducted 30-minute long, semi-structured interviews with ten participants to understand their attitudes toward privacy regarding the Snackbot, a social workplace robot [4]. We chose to study a workplace robot as it operates in both public and private spaces, and interacts with different types of users. The Snackbot is equipped with a fairly standard set of sensors for a social robot and includes two cameras, a microphone, two laser scanners, and an autonomous navigation system.

HRI'11, March 6–9, 2011, Lausanne, Switzerland.
ACM 978-1-4503-0561-7/11/03.

The interview session consisted of two parts. In the first part, we probed participants' initial understanding and perceptions about the robot using a one and half minute long video of the Snackbot (Figure 1). In the second part, we probed participants' attitudes toward accidental recording using a ten second long video of participants walking toward the interview room in a hallway. The participants' responses were transcribed and categorized according to privacy topics relating to sensing and data collection.

3. RESULTS

3.1 Initial understanding of the robot's recording capabilities

The interview results show that very few participants could make sense of the robot's data collection capabilities after watching the Snackbot video. As the robot verbally communicated with a user in the video, most participants inferred that the robot could understand users' speech. However, very few participants could identify the other sensors that the robot had (e.g., its cameras) or locate those sensors on the robot. Once the interviewer explained the types of sensors that were embedded in the robot, the participants were most surprised by Snackbot's omni-directional camera, which is situated on top its head, and were surprised that it could sense 360 degrees around the robot. The participants did not expect for the robot to see behind its back without turning its head.

When asked about their impressions and concerns about the robot, none of the participants expressed any privacy concerns related to personal data collection. This observation is consistent with ones made in privacy-related HCI research, where users were not able to estimate potential risks associated with their use of various interactive mobile technologies [3].

Even though the participants did not bring up this issue in their initial report, when asked whether the robot was recording, only a few participants recognized that the robot was recording audio and video, though they reported that this was likely done for performance improvement or security. Other participants reported that they did not think that the robot was recording any part of the user interaction at all.

3.2 Attitudes toward data recording

All of the participants said that they would not be concerned about any recordings of their interaction, as long as they were informed and aware that the robot was recording the interaction. They reported that they were used to surveillance cameras in public spaces, and treated the recording done by the robot as similar to the videos captured by security cameras.

However, participants' attitudes varied in regards to accidental recordings, i.e., recordings of a user that can occur when the robot navigates around or interacts with other primary users. Half of the participants reported that, if there was some notification of such a possibility (e.g., akin to a sign on the wall indicating the presence of security cameras), then they would be more comfortable with accidental recordings. The participants expressed that, because the robot operated in the workplace, it is unlikely that they would engage in behaviors that they should not be doing anyways. On the other hand, the other half of participants expressed concerns about the potential misuse of accidentally recorded videos. They expressed that such recordings could be used out of context, such as to unknowingly track a user's locations and routines. One participant reported concern about whether such recordings could occur when the robot is not in the line of sight. All of the participants expressed that they would want to be notified whether they were accidentally recorded by the robot.

3.3 Distinction between data and information

When describing the robot's data collection capabilities, most participants did not make the distinction between data and information. For example, most participants did not make any distinctions between pure sound recordings (i.e., recording the raw speech input) and a more processed speech recording (i.e., recording only keywords). However, a few participants expressed concerns about the robot being able to process certain elements of their interaction (e.g., the time and location) to infer meaningful information about the users. For example, one participant expressed that if the robot was roaming in the hallway in the morning every day, over time it might learn when he comes to his office, when he takes break, etc.; when compared to a coworker, the robot does not forget what it observes. He was concerned that these inferred patterns could be used by his boss or some other party in an unintended way.

4. DISCUSSION AND FUTURE WORK

The preliminary interview results showed that, regardless if they were the primary or secondary user, users were not able to accurately identify the types of data that could be collected by Snackbot. Few were able to make the distinction between what the robot sees/hears (i.e., sensed data) vs. what the robot knows (i.e., inferred information). These results suggest that the robot needs to accurately communicate the robot's data collection capabilities and how it constructs information/knowledge at multiple levels. One important factor to consider is that an anthropomorphic form can mislead/bias users' understanding about the robot's recording capabilities. If the robot is human-like, people might not expect the robot to have certain capabilities (e.g., being able to see objects behind the robot).

Future work will include further examining the perceptions of risk that were revealed in this study and, in particular, to understand how this compares with other types of data collection methods. In addition, more work will be done to investigate the different modalities and levels of control that users can have over their collected data.

5. REFERENCES

[1] Bellotti, V., and Sellen, A. (1993). Design for privacy in ubiquitous computing environments. *ECSCW'93*.

[2] Denning, T., Matuszek, C., Koscher, K., Smith, J. R., and Kohno, T. (2009). A spotlight on security and privacy risks with future household robots: Attacks and lessons. *Ubicomp'09*.

[3] Iachello, G., and Hong, J. (2007). End-user privacy in human-computer interaction. Foundations and Trends *Human-Computer Interaction*, *1, 1*.

[4] Lee, M. K., Forlizzi, J., Rybski, P. E., Crabbe, F., Chung, W., Finkle, J., Glaser, E., and Kiesler, S. (2009). The Snackbot: Documenting the design of a robot for long-term human-robot interaction. *HRI'09*.

[5] Solove, D. J. (2004). *The digital person: Technology and privacy in the information age*. NYU Press.