Walking Away from the Robot: Negotiating Privacy with a Robot

Trenton Schulz
University of Oslo
Postbox 1072 Blindern
0316 Oslo
Norway
trentonw@ifi.uio.no

Jo Herstad
University of Oslo
Postbox 1072 Blindern
0316 Oslo
Norway
johe@ifi.uio.no

Privacy is often applied as an abstract concept in law and regulations. In everyday life, negotiating what information to share with whom, where, and at what times, and in what situations may be a challenge at home and in public space. We apply Palen and Dourish's framework for understanding and discussing privacy to a setting of living with moving robots at home. We compare different ways sensors might be placed in a home environment, and what role proxemics, or motion technologies might have for the negotiation of privacy. By highlighting the role of the place and movement of the sensors, we discuss concrete privacy issues that are emerging with networked robot technologies at home. We hope to contribute new ways of thinking to users, designers, and analysts for creating and using mobile, networked technologies in domestic places.

privacy, robots, sensors, Internet of Things, human-robot interaction, movement

1. INTRODUCTION

In the past, when we were looking for privacy, we might seek out an area where no one was. If it wasn't possible to find an area devoid of people, we might draw curtains, close doors and windows, etc., to achieve our privacy. We can still do this today, but this may include turning off a telephone, computer, and other connected devices to truly "unplug" and get some privacy.

Privacy is beyond a single person. It involves a broad range of concerns within legislative practices, social practices, digital architecture, domestic and urban architecture. The activities of regulating our personal space, moving away from others or coming closer, opening doors, or avoiding others are privacy performed in practice during our everyday life. Yet as we live with more and more networked devices and services containing sensors, the question of privacy is increasingly a concern for the HCI research community and the public at large.

Most people reside in private homes. Traditionally, we feel the home is a place where we are private and enjoy full privacy. But modern, networked technologies with sensors are entering the home and challenging the privacy of residents.

Yet networked technology at home is not new. The fixed-line telephone, with microphone sensor and keypad (or rotary dial) that senses and transmits audio and control signals is such a device most of us are familiar with. The fixed-line telephone has several characteristics: (*a*) It is placed at a fixed place in the home, (*b*) It is visible to the resident when the sensors are on or off, and (*c*) during use of the telephone, the person is provided with a *side-tone*, indicating that the audio sensor is active; the rotary dial or key presses generate sound to communicate the number dialed.

On the telephone, a person is in control of (*a*) *where* the sensors are, (*b*) *when* the sensors are active or on and sensing, (*c*) *what* kind of data or information that is sensed, and to some extent (*d*) to *whom* the sensed data is distributed. These ways of living at home with sensors are challenged with more networked technologies entering the domestic place.

Networked technology can help us stay in touch and contact people when we need help. Yet this technology can cause issues with privacy and make us feel as if we are always being watched. In the area of the Internet of Things and cyber-physical systems, every object will talk with each other, and this will give us new ways of interaction, processing, and solving problems, but this also opens us up

Proceedings of British-HCI 2017

to new ways of being watched, uncertainty of how the data is being used, and how secure it is. With *smart homes*, sensors can communicate with each other via networking throughout the house and can help keep us safe, save electricity, or control parts of the environment. But in exchange, we need to provide information to these devices or alternatively the companies sitting behind the devices. For people that may want to live at home longer, all these sensors in their home may be required for welfare services to work.

In this paper, we look at what role the placement of sensors have for the control of what is sensed and possibly analyzed and recorded, and how we can negotiate our privacy with the services provided. Sensors can be positioned in various places in a home environment. We can put them into three categories based on their location.

Sensors can be fixed and stationary in the house
: *Examples*: PIR sensors for detecting human movement or microphones for recording orders. The resident can move around and—depending on the coverage of the fixed, stationary sensors in the home—the residents actions will be detected and recorded.

Sensors can be worn on the person's body
: *Examples*: motion sensors on watches, or audio sensor in smartphones placed in pockets and hands of residents. The resident can move around with the sensor, and of course put it away somewhere in the home.

Sensors can be placed on a robot
: *Examples*: camera or distance sensors on vacuum cleaners that move with the robot. The resident can move in relation to the robot, and get closer to it or move further away.

In these categories, some items are common among the sensors. They can be *visible* to the person, or they can be hidden. The sensors can potentially be turned *on and off*. Finally, the person can be informed about *what the sensors detect, record, and transmit*. The boundaries between categories also blur. For example, the smart phone can be worn on or about the body, but also placed at dedicated places in the environment.

Warren and Brandeis (1890, p. 195) write about the dangers of technology and privacy:

> Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops."

From these early discussions on the conditions for protecting privacy and ways of regulating privacy by law, there is an increasing focus on privacy as our everyday lives are partly lived on-line. The list of mechanical devices from 1890 is lately extended by robots in domestic places that move about with sensors—more or less autonomously—from room to room at home.

Most of this technology is stationary. In a smart home scenario, most items are sitting in one spot or are mounted at a certain point. This makes it necessary to put things all over the house to get sufficient coverage of the area. This can lead to an invasion of privacy where even areas like the bathroom are equipped with sensors for the sake of keeping someone safe.

Instead of adding sensors through the entire home; sensors could be in one place, for example on a robot. The robot can be combined with sensors like an infrared camera or laser guidance that can offer some anonymity. This robot would still have the role of being an assistive technology for people that want to live at home. But a robot that can move offers new opportunities. Instead of feeling like always being watched with sensors all over the house, people living at home know where the robot is. People could even ask the robot to leave if they felt that they wanted privacy for a while.

2. ROBOTS AT HOME

Many governments want to limit health costs in the future. One way of achieving this is to have people live longer at home independently as they grow older. Many of the proposed solutions for this have to deal with assistive technology that can help the person by monitoring vital statistics, reminding the person about appointments or taking medicine, contacting health professionals or family, etc. Lots of solutions are built on top of a smart home, where different sensors are around the home.

We are investigating using a robot that will be working with the elderly in their homes. We are in the phase of gathering information and requirements from the elderly, and we are looking at the possibility of adding sensors to help monitor different characteristics and health signs. This will later be combined with possibly guessing behavior with a goal towards early warnings about danger and keeping the person healthy in general. Some of these sensors require the robot to be a certain distance from the person. A robot may offer a better chance for privacy as the sensors are only on the robot instead of installed around the house.

3. RELATED WORK

As more devices are being introduced for the smart home, the security and privacy of the smart home is receiving more scrutiny. Though each smart home is different, they likely contain devices and sensors that help the home do things or assist the people at home. This brings up issues of trusting the device and assuming that people in the smart home can preserve their privacy (Schulz et al. 2014). Though not focusing on home, Fritsch, Groven, and Schulz (2012) identified different strategies one could use when interacting with different items where one cannot determine if one can or should trust the item.

Introducing a robot into a home can bring new problems. Robots need sensors to find their place in the environment or react to it. These sensors can gather different types of information, such as recording an image or audio. Depending on how the robot is set up, the information captured by the sensors may be sent over the network to other computers to give the robot more computing power than it might otherwise have due to its size or power constraints (Kanda and Ishiguro 2012). This can result in breaching the privacy of people in the area working with the robot.

Robots and privacy is a topic that has not been researched much. Calo (2010) presents an overview of the privacy issues around surveillance and the fact that we act differently around anthropomorphic social robots. Peter H. Kahn et al. (2007) and Feil-Seifer, Skinner, and Matarić (2007) proposed benchmarks for evaluating human-robot interaction that included privacy. Syrdal et al. (2007) found different opinions about what should be recorded from the people they interviewed for a robot in a home scenario. No one they interviewed was completely comfortable with a robot recording the information, but tolerated it if it was for an obvious purpose.

Depending on the robot's design, its sensors may not be obvious for everyone. A study by Lee et al. (2011) showed that people were not aware of the sensing capabilities of the robot (for example, that it could see behind itself) or a difference in what it collected and what it processed. Not fully understanding the sensors on a robot may even extend to the cameras on a robot. Calo (2011) posits that drones carrying cameras in public areas could highlight citizen's need for privacy and make it easier to recognize privacy. Yet Caine, Šabanović, and Carter (2012) ran an experimental study with a camera, a stationary robot, and a mobile robot to see how older adults changed their behavior to preserve their privacy. Caine, Šabanović, and Carter found that the older adults exhibited the most privacy-preserving behaviors when a camera was used and not a mobile robot.

Much of the current research with robots and privacy has focused on telepresence or teleoperated robots. These robots are operated by another person and allows the person to be present and perform tasks in the environment where the robot is located. Research here has focused on obscuring the environment from the robot operator. Butler et al. (2015) looked at people's perceptions of privacy and how well different types of video filters would affect the operator's ability to perform tasks. Other types of filters have also proven effective (Hubers, Andrulis, Scott, et al. 2015; Hubers, Andrulis, Smart, et al. 2015). M. Rueben et al. (2016) experimented with different interfaces for marking objects that should remain hidden to a robot's camera. Matthew Rueben et al. (2017) found that informing people that the robot was being operated by someone known versus unknown was important to a person's privacy concerns and what the robot did.

ICT related privacy research often focus on technology and ways of implementing technologies, see Bellotti and Sellen (1993). Palen and Dourish (2003) have proposed a framework for a more nuanced understanding of privacy in a networked world. Building on the work of Altman (1975), they identify three boundaries for negotiating information disclosure:

Disclosure boundary This is the boundary of what you tell others and what you keep to yourself. For example, writing opinions about a subject in a public forum or wearing a t-shirt of a band you enjoy.

Identity boundary This is the boundary for the different roles we have in our lives. For example, in some areas we are an employee, other areas an enthusiast, and others a friend. Each of these roles have different kinds of information we share or don't share.

Temporal boundary This boundary controls how information is handled over time. For example, knowing you borrowed a book from the library versus knowing your entire history of books you have borrowed from the library.

Palen and Dourish provide several examples to show how different goals need to be negotiated to maintain privacy, while making it possible to use the network. Their examples show the unintended consequences of using a network environment—such as their example of a potential downsizing in a company being leaked because all the meeting rooms are booked by the HR department.

Palen and Dourish's framework has been used in other situations. Holone and Herstad (2010) used the framework when mapping areas for accessibility issues and sharing the maps.

4. USING A PRIVACY FRAMEWORK WITH A MOVING ROBOT IN THE HOME

Here we investigate how a person can negotiate privacy with a robot in the home using the framework proposed by Palen and Dourish. Even without a final robot selected, this privacy framework is an exercise for looking at privacy issues and part of a foundation in *privacy by design* (Langheinrich 2001).

Yet it is easier to visualize privacy issues if we have an idea of the capabilities of the robot. So, let's assume that the robot can move in the house and that the robot has sensors that can track the person via infrared (Kido et al. 2009) and wide-band sensors (Tømmer, Kjelgård, and Lande 2016); the latter it uses for measuring the pulse of the person when the robot is close enough to the person.

4.1. The disclosure boundary

For our project, the robot is to be in the home to help someone stay at home longer. This means that some information must be disclosed to the robot, for example the person's age or what problem's the person has (medical or physical) that the robot could help out with or monitor. Some may accept the robot having this information if it means they can stay home longer. Yet the robot is also staying in the home with the person and it can start picking up other information through its sensors. Some of this information can be helpful and timely, such as monitoring heart rate and notifying medical staff when it drops low. Other times, having the robot at home may disclose a person's habits to others, like the person's secret addiction to chocolate. Having respect for this person's boundary while still looking out for the person's better health is necessary.

4.2. The identity boundary

Palen and Dourish discuss how technology *mediates* our interaction between the technology and the world and how this blurs the line between what is private and public. A robot at home contributes to this blurring. The robot is set up as something to help the person. We may consider the person in a patient role and the robot as a servant. But while the robot is present, its sensors may detect people visiting where the person takes on other roles (e.g., a parent, grandparent, club member, or friend). The robot should handle these visits and let the person play different roles without fear of different identities being leaked.

4.3. The time boundary

Since the robot stays in the home over an extended period, the robot can build a more complete picture of the person and track activities and other disclosures over time. Though the robot may be around the person more, there are several questions we can ask that can give us an idea about how big this boundary is: Whom are we sharing with? Where? At what times and in what situations, and how long? Information about everyday home activities that used be ephemeral is potentially made permanent and may be used at later times.

4.4. Walking away

One of the features we want to explore is the robot moving in the house (as will the people). In essence, someone could walk away from the robot or send the robot away to get some privacy. This changes the dynamic of sensors, especially if we work with the idea that the sensors are on the robot.

Movement affects the boundaries named above. For example, a person moving to another part of the home or asking for the robot to go to another part of the house could help strengthen the disclosure boundary as the robot would not have access to the information. It would also strengthen the identity boundary since the robot would not have the whole picture of the different roles. The time boundary would also be affected since the robot would not have the whole story.

Since walking away from the sensors on the robot is possible, let's compare with the other sensor configurations named in Section 1. Depending on where the fixed sensors are placed in a house, it might be possible to walk away from the them as well, but it might mean parts of the house are not ever available for privacy or privacy is limited to a very small part of the house. For the other configuration, it is difficult to walk away from a sensor worn on the person. The sensor could be removed, but this might trigger an alert that could result in the privacy being short lived.

Walking away from the robot gives us an easy to understand control over our privacy. It also can make the robot walk to us. The robot's movements can be animated to make it obvious if the robot is searching, when the robot has found us, if it's observing, and when we have moved out of range. This animated movement will give the robot some personality and give us an idea of what the robot is doing. This movement, animation, and control over privacy is something we hope to investigate in future work.

5. CONCLUSION

We have used the perspective on privacy from Palen and Dourish to investigate the negotiation of privacy at home with robots. Looking at this negotiation shows why it is important to practice privacy by design to make sure that people's information remains secure and their privacy is preserved.

Bellotti and Bly (1996) looked at how movement beyond the desktop computer was important for the product design team. Movement adds a different type of interaction and a possibility of negotiating privacy in new ways. Walking away from the robot or asking the robot to leave gives a person a direct physical way of seeing how much is being recorded. The robot also could serve as a means of visualizing that recording is taking place. People would be reminded that when the robot is present, they may be recorded. This can easily be forgotten when sensors are hidden in the environment.

This "out of the robot's sight, out of surveillance" model isn't perfect. Some types of sensors that can see through walls may still raise issues of surveillance. Some sensors provide some anonymization, but leak other types of information—for example, an infrared picture doesn't give us features of the face, but it can tell us about the person's gender. Also while some sensors may be blocked, there may be other ways of getting the data, as demonstrated in the film *2001* (Kubrick 1968) where the astronauts successfully stop the HAL-9000 from hearing their conversation, yet HAL is still able to read their lips. Work would need to be done to show the capabilities and direction of the sensors to help inform what is being collected. Overall, this movement method may be useful and instructive for the people living at home with a robot.

5.1. Acknowledgments

This work is part of the MECS project funded by the Norwegian Research Council IKTPluss Program (Grant agreement no: 247697). We would also like to thank Mark Summerfield and Diana Saplacan for proofreading drafts.

REFERENCES

Altman, Irwin. 1975. "The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding." Accessed March 9, 2017.

Bellotti, Victoria, and Sara Bly. 1996. "Walking Away from the Desktop Computer: Distributed Collaboration and Mobility in a Product Design Team." In *Proceedings of the 1996 ACM Conference on Computer Supported Cooperative Work,* 209–218. CSCW '96. New York, NY, USA: ACM. Accessed February 3, 2017.

Bellotti, Victoria, and Abigail Sellen. 1993. "Design for Privacy in Ubiquitous Computing Environments." In *Proceedings of the Third European Conference on Computer-Supported Cooperative Work 13–17 September 1993, Milan, Italy ECSCW '93,* edited by Giorgio de Michelis, Carla Simone, and Kjeld Schmidt, 77–92. Springer Netherlands. Accessed March 28, 2017.

Butler, Daniel J., Justin Huang, Franziska Roesner, and Maya Cakmak. 2015. "The Privacy-Utility Tradeoff for Remotely Teleoperated Robots." In *Proceedings of the Tenth Annual ACM/IEEE International Conference on Human-Robot Interaction,* 27–34. HRI '15. New York, NY, USA: ACM. Accessed May 4, 2017.

Caine, K., S. Šabanović, and M. Carter. 2012. "The Effect of Monitoring by Cameras and Robots on the Privacy Enhancing Behaviors of Older Adults." In *2012 7th ACM/IEEE International Conference on Human-Robot Interaction (HRI),* 343–350.

Calo, Ryan. 2010. *Robots and Privacy.* SSRN SCHOLARLY PAPER ID 1599189. Rochester, NY: Social Science Research Network. Accessed May 9, 2017.

———. 2011. *The Drone as Privacy Catalyst.* SSRN SCHOLARLY PAPER ID 2340753. Rochester, NY: Social Science Research Network. Accessed May 8, 2017.

Feil-Seifer, David, Kristine Skinner, and Maja J. Matarić. 2007. "Benchmarks for Evaluating Socially Assistive Robotics." *Interaction Studies* 8, no. 3 (): 423–439. Accessed May 8, 2017.

Fritsch, Lothar, Arne-Kristian Groven, and Trenton Schulz. 2012. "On the Internet of Things, Trust Is Relative." In *Constructing Ambient Intelligence,* edited by Reiner Wichert, Kristof Laerhoven, and Jean Gelissen, 277:267–273. Communications in Computer and Information Science. Berlin: Springer Berlin Heidelberg.

Holone, Harald, and Jo Herstad. 2010. "Negotiating Privacy Boundaries in Social Applications for Accessibility Mapping." In *Proceedings of the 6th Nordic Conference on Human-Computer Interaction: Extending Boundaries,* 217–225. NordiCHI '10. ACM ID: 1868942. New York, NY, USA: ACM.

Hubers, Alexander, Emily Andrulis, Levi Scott, Tanner Stirrat, Ruonan Zhang, Ross Sowell, Matthew Rueben, Cindy M. Grimm, and William D. Smart. 2015. “Using Video Manipulation to Protect Privacy in Remote Presence Systems.” In *Social Robotics,* edited by Adriana Tapus, Elisabeth André, Jean-Claude Martin, François Ferland, and Mehdi Ammi, 245–254. Lecture Notes in Computer Science 9388. Springer International Publishing. Accessed October 18, 2016.

Hubers, Alexander, Emily Andrulis, William D. Smart, Levi Scott, Tanner Stirrat, Duc Tran, Ruonan Zhang, Ross Sowell, and Cindy Grimm. 2015. “Video Manipulation Techniques for the Protection of Privacy in Remote Presence Systems.” In *Proceedings of the Tenth Annual ACM/IEEE International Conference on Human-Robot Interaction Extended Abstracts,* 59–60. HRI’15 Extended Abstracts. New York, NY, USA: ACM. Accessed May 4, 2017.

Kanda, Takayuki, and Hiroshi Ishiguro. 2012. *Human-Robot Interaction in Social Robotics.* Google-Books-ID: Svid3OuCOSkC. CRC Press.

Kido, S., T. Miyasaka, T. Tanaka, T. Shimizu, and T. Saga. 2009. “Fall Detection in Toilet Rooms Using Thermal Imaging Sensors.” In *2009 IEEE/SICE International Symposium on System Integration (SII),* 83–88.

Kubrick, Stanley, dir. 1968. *2001: A Space Odyssey.* In collaboration with Keir Dullea, Gary Lockwood, William Sylvester, and Daniel Richter. Film.

Langheinrich, Marc. 2001. “Privacy by Design — Principles of Privacy-Aware Ubiquitous Systems.” In *Ubicomp 2001: Ubiquitous Computing,* edited by Gregory Abowd, Barry Brumitt, and Steven Shafer, 2201:273–291. Springer Berlin / Heidelberg.

Lee, Min Kyung, Karen P. Tang, Jodi Forlizzi, and Sara Kiesler. 2011. “Understanding Users’ Perception of Privacy in Human-Robot Interaction.” In *Proceedings of the 6th International Conference on Human-Robot Interaction,* 181–182. HRI ’11. New York, NY, USA: ACM. Accessed March 20, 2017.

Palen, Leysia, and Paul Dourish. 2003. “Unpacking ”Privacy” for a Networked World.” In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,* 129–136. CHI ’03. New York, NY, USA: ACM. Accessed February 17, 2017.

Peter H. Kahn, Jr, Hiroshi Ishiguro, Batya Friedman, Takayuki Kanda, Nathan G. Freier, Rachel L. Severson, and Jessica Miller. 2007. “What Is a Human?: Toward Psychological Benchmarks in the Field of Human–robot Interaction.” *Interaction Studies* 8, no. 3 (): 363–390. Accessed May 8, 2017.

Rueben, M., F. J. Bernieri, C. M. Grimm, and W. D. Smart. 2016. “Evaluation of Physical Marker Interfaces for Protecting Visual Privacy from Mobile Robots.” In *2016 25th IEEE International Symposium on Robot and Human Interactive Communication (RO-MAN),* 787–794.

Rueben, Matthew, Frank J. Bernieri, Cindy M. Grimm, and William D. Smart. 2017. “Framing Effects on Privacy Concerns About a Home Telepresence Robot.” In *Proceedings of the 2017 ACM/IEEE International Conference on Human-Robot Interaction,* 435–444. HRI ’17. New York, NY, USA: ACM. Accessed April 25, 2017.

Schulz, Trenton, Kristin Skeide Fuglerud, Henrik Arfwedson, and Marc Busch. 2014. “A Case Study for Universal Design in the Internet of Things.” In *Universal Design 2014: Three Days of Creativity and Diversity,* edited by Héctor Caltenco, Per-Olof Hedvall, Andreas Larsson, Kirsten Rassmus-Gröhn, and Bitte Rydeman, 45–54. IOS Press.

Syrdal, Dag Sverre, 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 *Proc. Workshop Human Implications of Human–robot Interaction, Association for the Advancement of Artificial Intelligence (AAAI’07),* 28–33. Accessed March 20, 2017.

Tømmer, M., K. G. Kjelgård, and T. S. Lande. 2016. “Body Coupled Wideband Monopole Antenna.” In *2016 Loughborough Antennas Propagation Conference (LAPC),* 1–5.

Warren, Samuel D., and Louis D. Brandeis. 1890. “The Right to Privacy.” *Harvard Law Review* 4, no. 5 (): 193–220.