Privacy and Healthcare Robots – An ANT Analysis

Christoph Lutz

BI Norwegian Business School

Department of Communication & Culture

Nydalsveien 37, NO-0484 Oslo

christoph.lutz@bi.no

University of Leipzig

Institute of Communication and Media Studies

Burgstrasse 21, DE-04109 Leipzig

christoph.lutz@uni-leipzig.de

Aurelia Tamò

University of Zurich

Chair for Information and Communication Law

Rämistrasse 74/49, CH-8001 Zurich

aurelia.tamo@uzh.ch

Visiting: Harvard University

Berkman Center for Internet & Society

23 Everett St #2, Cambridge, MA 02138

Abstract

The privacy implications of social robots are far-reaching and concern both informational and physical privacy. In this contribution we address the topic of healthcare robots and privacy. We use actor network theory (ANT) to shed light on the privacy implications of healthcare robots from a specific theoretical point of view. ANT is a descriptive, constructivist approach that takes into account the agency of objects, concepts and ideas as well as the relationality of technology and the social. It has been applied to complex technological innovations, such as e-health systems. We use some of the main concepts of ANT—actants, translations, tokens/quasi-objects, punctualization, obligatory passage point—to "map" the privacy ecosystem in robotic healthcare technology, thereby analyzing the complex interplay of robots and humans in that context. Altogether, our contribution shows that ANT is a fruitful lens through which to study the interaction between humans and (social) robots because of its richness of useful concepts, its balanced perspective which evades both technology-determinism and social-determinism, and its openness towards new connected technology.

Keywords: privacy, healthcare robots, actor network theory, HRI

Introduction

Artificial intelligence and robots reach higher and higher capacity levels every year. At the same time, they experience massive diffusion and will continue to be adopted to a large extent in the coming years (Gupta, 2015; van den Berg, 2016). Robots are already heavily used in industrial settings, and increasingly so also in healthcare, for service tasks and in households (Lin, 2012). Social robots—those that interact with us in some way—register our habits and attitudes, affecting our sense of intimacy, privacy, bonding and emotional support (Syrdal, Walters, Otero, Koay, & Dautenhahn, 2007). Studies in the field of human robot interaction have shown that humans tend to anthropomorphize social robots, which substantially increases the pervasiveness of such technology compared with other connected technology such as tablets or smart fridges (Darling, 2012; Turkle, 2011). In addition, by definition, robots possess real-life agency and limited autonomy, *i.e.*, they not only collect and process information but they also act upon it by physically reaching out into the world (Bekey, 2012; Lutz & Tamò, 2015).

This further increases their pervasiveness and creates the potential for physical damage. With such real-life agency comes an unprecedented potential for access to personal rooms and surveillance (Calo, 2012). Taken together and coupled with a lack of awareness of how such technology works (Lutz & Tamò, 2015), these aspects threaten to endanger consumers' privacy and to substantially limit their control of sensitive data (such as emotional states, health information and intimate relationships) when they interact with robots. Summed up, the privacy implications of social robots are far-reaching and concern both informational (Felzmann, Beyan, Ryan, & Beyan, 2015; Syrdal, Walters, Otero, Koay, & Dautenhahn, 2007) and physical privacy (van Wynsberghe, 2013).

In this contribution we address the topic of healthcare robots and privacy. Our choice of healthcare robots over other (social) robots comes from the fact that they often deal with extremely sensitive information and with very vulnerable population groups, *i.e.*, the elderly and/or severely ill individuals (van Wynsberghe, 2013). In this sense, they present a "worst case scenario" for privacy where potential privacy intrusions are especially severe. We use actor network theory (ANT) to shed light on the privacy implications of healthcare robots from a specific theoretical point of view. ANT strives to be a descriptive, constructivist approach that takes into account the agency of objects, concepts and ideas as well as the relationality of technology and the social (Latour, 1987). It has been applied to complex technological innovations, such as e-health systems (e.g., Muhammad & Wickramasinghe, 2014). We will use some of the main concepts of ANT to "map" the privacy ecosystem in robotic healthcare technology, thereby analyzing the complex interplay of robots and humans in that context.

The paper contains three main parts plus an introduction and conclusion. In the first main part, we provide background information on the topic of healthcare robots, discuss their application and elaborate on why this technology is gaining momentum and is meant to stay. In the second main part, we look at how such robots potentially disturb individuals' privacy. We consider both informational and physical privacy and discuss the privacy implications of healthcare robots with an application scenario for both cases. In the third main part, we apply ANT to the topic of privacy and healthcare robots. To do so, we briefly explain the core constructs of the theory and then apply them to the issue at hand. ANT provides a suitable framework to describe the privacy ecosystem in the context of healthcare robots. The introduction of the paper briefly opens up the discourse, states the goals and contributions of the paper and explains the structure. The conclusion summarizes the key findings, names salient implications for theory and practice, and points to the limitations of our approach. The main

contribution of the paper is twofold. On the one hand, we show how privacy issues are at play for the emergent technology of healthcare robots, both informationally and physically. The application scenarios illustrate the serious privacy repercussions of the employed technologies. On the other hand, we contextualize the notion of privacy for healthcare robots by applying ANT. This reveals how a complex and fluid network of concrete and abstract actors is at play and forms the robotic privacy ecosystem.

Robots in Our (Nursing) Homes and Hospitals

Robots are gradually moving into our homes and institutions. Future households, nursing homes and hospitals will be more densely populated with social robots interacting with family members and patients. The adoption of robots as new household members at home as well as the delegation of specific nursing tasks to robots in nursing homes and in hospitals importantly shapes our attitudes towards our mechanical friends. While pleasant interactions will promote the use of social robots, unpleasant ones are likely to have a deterrent effect. In particular, the interaction in households—assumed to be more relaxed and fun—will shape the way individuals will gradually accept robots in a healthcare setting.

The yearly Consumer Electronics Show displays future household robots. One example is Furo-i Home.[1] Furo-i comes on wheels, is equipped with a Samsung tablet displaying the droid's friendly face and interacts with smart devices connected to the Internet. Users can thus use voice commands to order Furo-i to control the devices it interacts with. They can ask Furo-i, for example, to turn on the light, coffee machine or heater. Via multiple sensors and cameras Furo-i explores the environment it is in, the temperature of the room and the people it interacts with (via facial recognition). It can be programmed to help children with their homework, look after what they are doing, and, should unexpected events occur, alert parents with a message. It can also wake up the kids or the parents, remind elderly people to take their medicine and guide them throughout the rest of their schedule (*e.g.*, ensuring that they do not miss a doctor's appointment). Furo-i is thus a helpful addition to the household environment and its convenience is likely to be a critical characteristic in the adoption of such household robots. It has even been predicted that social robots could replace pet ownership since robot pets would have the benefit of being considerably cheaper while still allowing us to bond with them as we would with animals (Ackerman, 2015). While this might still be a futuristic scenario, the

[1] http://www.myfuro.com/

potential close bonds between humans and anthropomorphic robot toys promotes the assumption that we could, and indeed would, treat such toys more as pets than as machines (Darling, 2016).

These developments in adopting household robots are also visible in the healthcare sector. Here the employment of robots can take multiple forms. Robots, for example, can be used as surgery assistants, for patient transportation and can also be used to provide ad hoc support to doctors and nurses. This paper restricts its focus to home healthcare robots which act as a form of personal assistance through patient monitoring. Examples of such home healthcare robots include therapy robots (*e.g.*, Paro for animal therapy or CosmoBot for the tailored treatment of disabled children)[2], monitoring robots (*e.g.,* Anybots[3] which monitor spaces and can be controlled from afar), or personal assistants (*e.g.,* the Furo-i mentioned above as well as robots which move inventory or elderly people out of the bed, *e.g.,* Riba).

A large potential market for healthcare robots exists with older patients who are more in need of assistance or with patients who have limited faculties of movement or communication.[4] However, home healthcare robots can be of use in other settings as well. For instance, a recent survey indicates that patients respond better to robots than tablet-computers when receiving healthcare instructions (Mann, MacDonald, Li, & Broadbent, 2015). These survey results show that when a robot, in contrast to a tablet-computer, asks a patient health-related questions or instructs them to perform either limited physical tests or relaxation exercises, patients have a more positive interaction with the robot (measured by length of interaction dialogue and positive emotions such as smiling). Also, patients tend to follow the instruction of robots more than the instruction of a tablet-computer (Mann, MacDonald, Li, & Broadbent, 2015).

The intention to use home healthcare robots depends on various factors, one of them being privacy concerns and the related trust which has been placed in the robot (Alaiad & Zhou, 2014). Since the benefits of home healthcare robots are far reaching, it is important that privacy concerns should not inhibit their adoption. The next chapter elaborates on the role which privacy can play in the adoption of home and healthcare robots.

---

[2] http://www.allonrobots.com/robotic-therapy.html
[3] https://www.anybots.com/products/
[4] http://www.hsi.gatech.edu/hrl/projects.shtml and http://www.hsi.gatech.edu/hrl/project_pr2.shtml

On Healthcare Robots and Privacy

Restricting the scope of the concept of privacy is vital, especially given its breadth and inclusion of multiple elements. To narrow down the notion of privacy used in this paper, we deliberately consider only individual and collective interests in the protection of privacy. Regulatory, economic or technical interests for privacy protection are not part of the research focus (Aeschlimann *et al*., 2015).

Multiple authors have distinguished different types and dimensions of privacy. One of the first, and certainly one of the most influential, definitions comes from Warren and Brandeis (1890), who defined privacy as "the right to be let alone". While this has been be a useful first step in defining the phenomenon, it is too simplistic and too heavily focused on the physical dimension of privacy (in the sense of freedom from intrusion into private spaces and of exemption from press coverage). With the advent of the Internet and other sophisticated information technology, the informational aspect of privacy has gained importance. Thus, the privacy discourse, especially in the legal area, is typically framed as an issue of data protection. Consequently, the vast bulk of privacy research in the context of the Internet and computer technology focuses on informational privacy and personal data as well as control over it (Smith, Dinev, & Xu, 2011). Here, the definitions of Westin (1967, p. 7)[5] and Altman (1975, p. 24)[6] are more appropriate as well as Petronio's (2002) privacy management theory (Margulis, 2011). We argue here that with the advent of robots, which have real-life agency as one of their defining characteristics (Bekey, 2012), physical privacy is again becoming more relevant.

In addition to physical and informational privacy, social privacy and psychological privacy have been distinguished as dimensions of the concept (Burgoon, 1982). Social privacy is concerned with control over interactions and both the proximity towards and distance between other individuals (Trepte & Reinecke, 2011). Physical and social privacy can overlap, for example in the context of intercultural face-to-face interaction where different cultures or social milieus have various levels of physical distance. Thus, bodily contact can be either seen as an intrusion of privacy or as a normal part of interaction. Finally, psychological privacy entails the "control over emotional and cognitive inputs or outputs" (Trepte & Reinecke, 2011, p. 60). In this article, we are more interested in informational, physical and social privacy than in psychological privacy. It must be said, however, that these dimensions of privacy are

[5] He defines privacy as "[…] the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. [Moreover] . . . privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means."
[6] He defines privacy as "the selective control of access to the self."

intrinsically intertwined and often coincide. For example, when a burglar breaks into a house and steals personal belongings, this is a violation of both physical and informational privacy. In the remainder of this section we will discuss the privacy implications of home healthcare robots for each dimension of privacy.

For concerns of *physical privacy*, the fact that a robot can react to its environment and move is significant. The robot, for instance, can enter bedrooms while the tenants are awake or asleep. It can also move around houses and flats, monitor the individuals present, and, via face recognition and/or social media data analysis, attribute those faces to certain identities. Here, the desire to retreat within a "safe", *i.e.,* unmonitored and "un-entered", space becomes again relevant.

Calo (2012) identifies three core privacy risks of robotic technology: surveillance, access, and social bonding. Two of these three forms are connected to physical privacy. Surveillance, in the context of robots, often involves a physical component as exemplified by drone spying in military contexts. Similarly, home healthcare robots could be (ab)used for surveillance purposes by the government, corporations or private citizens. One can imagine a scenario where security services install tracking software into such an ostensibly harmless robot to monitor the whereabouts and habits of suspicious subjects. Similarly, access can have physical repercussions if, for example, a robot involuntarily enters an individual's bedroom or bathroom while they were in an intimate situation. Compared with other advanced forms of information technology in healthcare settings, such as wristbands, smart phones or tablet-computers, the privacy consequences of robots are more far-reaching. This is because of their real-life (quasi)agency and higher degree of autonomy.

Connected to physical privacy is *informational privacy*. Social robots, including those in a healthcare context, can gather, analyze and act upon a vast body of data. The collection of identifiable user data (*e.g.,* names, date of birth, eating preferences and cultural taste), location data or other types of sensitive information is, at its root, an issue of informational privacy. According to Alaiad & Zhou (2014), informational privacy is the most relevant form of privacy with respect to the acceptance of robot technology. Other authors agree that information processing is one of the core aspects of robotics (Felzmann *et al.,* 2015). Thus, robots "do not just impact on the physical environment of their users or provide limited, task specific information, but control the informational environment for humans more comprehensively" (Felzmann *et al.,* 2015, p. 3).

In this sense, additional concerns beyond those raised in HRI studies occur. The tracking and profiling of users and bystanders through robots is one example, leading us to question what information is obtained and how this information is to be used. One can imagine a scenario where a healthcare robot collects information not only about the patient to whom it has been designated, but also collects information about other individuals, such as children, in the vicinity without their knowledge. A further issue in the field of informational privacy is the sharing of data with third parties for unintended and non-consensual purposes (Felzmann *et al.*, 2015). A study by Syrdal and colleagues (2007) showed that most participants felt uneasy when put in a scenario where robots had the power to disclose personal information, such as psychological or personality characteristics, to other individuals without their permission. They were also worried about the possibility of data about themselves being collected by robots of others, similar to concerns about drones (PEW, 2014).

The concept of contextual integrity or privacy in context (Nissenbaum, 2004) can be applied to informational and data privacy. We have to ask (1) to whom the data is communicated and whether this corresponds with the existing information norms in a given setting (it might be appropriate to pass medical information on to doctor but not to an employer) and (2) what conversations among individuals are recorded by the robot and how they are used. Robots' sensory capabilities and abilities to process real-time big data enable a multitude of services. For instance, in healthcare and elderly care, doctors and nurses can delegate particular duties to robots, such as reminding patients to take their medicine, checking patients' pulse rates, monitoring activities at home, monitoring eating habits as well as undertaking routine activities and social interactions (Felzmann *et al.*, 2015). However, the delegation of such tasks to healthcare robots "raises significant issues regarding the role and use of information that underlies such decision-making" (Felzmann *et al.*, 2015, p. 3).

As for *social privacy*, the human tendency to anthropomorphize social robots (*e.g.*, Breazeal, 2003; Duffy, 2003) becomes a privacy topic. Calo (2012) describes this aspect as social bonding. In its broadest form, privacy is the right of individuals to be "let alone" (Warren & Brandeis, 1890). Being "let alone" serves multiple interests. It enables individuals to, for example, retreat within safe boundaries, to psychologically evolve, to decide both what they share with others and what they believe, and to feel free from outward pressure. Trust plays an important role when we look at social privacy needs. Since healthcare is, to a large extent, a social setting with specific actors co-operating (see below), the element of communication and interaction should not be neglected. In a similar manner to virtual assistants on computers and

smartphones (such as Siri), social robots often have sophisticated speech recognition and language capabilities which enable interaction and the establishment of intimate relationships.[7] Given the human tendency to bond with robots in a fashion similar to human bonding with other people, individuals might be inclined to discuss very personal and delicate topics with a robot such as emotional states, feelings or even secrets. The robot, however, might not be designed to adequately deal with such sensitive topics. Healthcare robots, in this sense, could be seen by some people as counsellors rather than assistants or servants (Rabbitt, Kazdin, & Hong, 2015). As before, this "category" or sphere of privacy is interconnected with informational and physical privacy. Social interactions entail information and take place in a physical space. Thus, the topic of social privacy in the context of robots is strongly intertwined with informational and physical privacy.

Actor Network Theory (ANT), Robots and Privacy

ANT: Networks as a Method of Analysis

We rely on the Actor Network Theory (ANT) to describe privacy issues within the healthcare and robotics field. The next chapters will provide an overview of the ANT method of analysis, followed by the application of the theory to healthcare robots and a mapping of privacy-related issues.

Actor Network Theory (ANT) was developed in the mid 1980s by the sociologists Michel Callon, Bruno Latour and John Law. The theory argues that technology and the social environment interact with each other, forming complex networks. These networks[8] consist of multiple relationships between the social, the technological or material, and the semiotic. In other words, according to ANT, the world cannot simply be divided into either social or material aspects and any analysis of both aspects separately from each other is doomed to fail. Rather, ANT stresses the capacity of technology to be an actor in and of itself, one which influences and shapes other social relations. ANT sees material objects as an element of a network.

[7] This topic has been taken up by Hollywood and science-fiction writers. The movie "Her" is a good example for a narrative of the bonding between artificial intelligence and humans.

[8] It is important to recognize that the concept of a network in ANT does not refer to the analysis and explanation of existing networks such as Facebook friend networks, kinship networks or intra-organizational networks, as would be the case in structural sociology and social network analysis. Rather, ANT describes a method with which something can be described.

Illustrating the relationship between objects (amongst both other objects and humans) is the main aim of ANT.

In this sense, ANT is more of a descriptive framework than an explanatory theory. Instead of explaining relationships in terms of cause-and-effect, ANT describes the interactions between units or elements. It treats objects and subjects, both human and non-human, with the same vocabulary (the terminologies used will be explained below). By focusing on the interaction between various actors and concepts, the ANT framework describes the ordering of technological, social, and organizational developments. In the words of Latour: "Network is a concept, not a thing out there. It is a tool to help describe something and not what is being described." (Latour, 2005, p. 131). As the term "network" illustrates, the interesting part of this descriptive process is the interaction, energy, flow and link between different actants (contrary to the human actors themselves). An actant can be anything - from a robot to a human being - which "influences the turn of events" in a particular setting (Krieger & Belliger, 2014, p. 92).

> *"The imperative of ANT is simply to 'follow the actors' and not attempt to look behind, above, or beneath them in order to discover some kind of conditioning factors operating, so to speak, behind their backs and making them do what they do."* (Krieger & Belliger, 2014, p. 59)

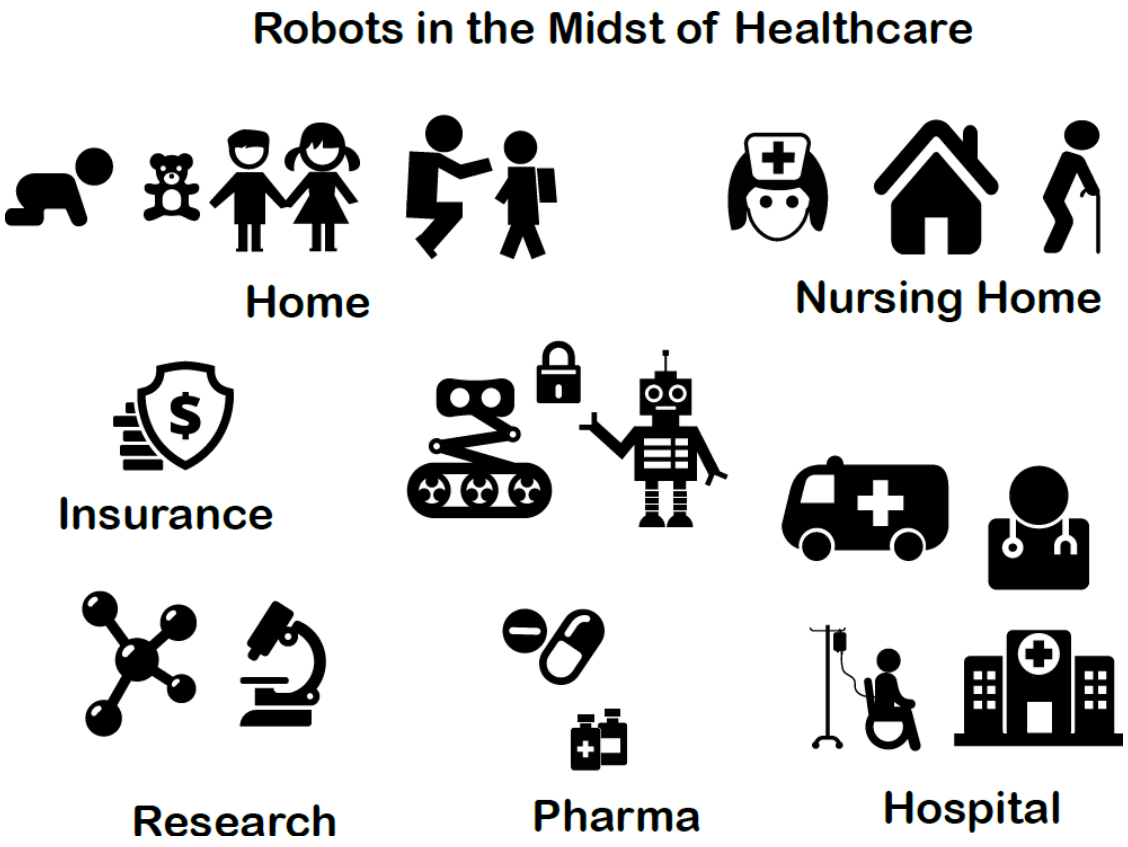
Latour (1994) illustrates ANT with a famous case study on guns. He argues that the gun itself can be seen not only as an object but also as an actant and, as an actant, a gun pushes humans to pull the trigger. In this sense, humans and guns transform one another when combined - the object itself cannot kill. Humans might not feel the urge to kill and might not be able to do so, either with other weapons or with their bare hands. When in combination - the gun in an individual's hand - this initial setting changes: the interaction creates a "gunman". The feeling of a gun in their hands transforms humans as they enter a relationship with their gun (Latour, 1994). They become gunmen, which in itself is an actor-network. Therefore, Latour argues that the responsibility for actions must be shared among actants in a network.

What ANT Offers for the Analysis of the Robot-Patient-Interaction

In the context of healthcare robots, the network encompasses not only robots and users, but also doctors, nurses, other individuals present in a home and technologies such as sensors, movement/agility mechanisms and design features of robots. Together, they form one network

(*e.g.*, "a robotic home healthcare environment"). ANT attempts to explain how those material-semiotic networks come into existence and how they act as a whole.

The following figure illustrates the network in a healthcare robotics setting but is by no means exhaustive.



In this paper we look at the following actants: (1) individual actors (children, parents or the elderly), (2) home healthcare robots (for therapy, monitoring or assistance), (3) doctors and nurses, (4) insurances, (5) pharmaceutical companies, and (6) cloud based applications and software (cloud robotics). The latter refers to the process of outsourcing robots' data processing to the cloud. Cloud processing frees robots from previous computing constraints and enables the processing of gigantic amounts of data to occur in real time. Coupled with advances in big data analytics, robots now have much more substantive databases at hand and can thereby react to a wide set of challenging situations (Gupta, 2015; Felzmann *et al.*, 2015; van den Berg, 2016). This development importantly supports the massive diffusion of robots in the near future because it "greatly increases the amount and variety of tasks a single robot can complete" (van

den Berg, 2016, p. 5). Hence, by connecting robots to the Internet and enabling the sharing of what robots have learned to do with other robots, cloud robotics will expand the abilities of robots and increase their functionality. However, connecting robots to the Internet also opens up security risks (*i.e.,* by outsiders gaining access to the robots) as well as potential privacy breaches or exploits (van den Berg, 2016).

In the following paragraphs we will describe the relationships between the different actants in the network by referring back to some of the key terms in ANT (Muhammad & Wickramasinghe, 2014).

Actants. Frequently used terms in ANT are "actor" and "actant". The former relates mostly to human actors while the latter describes the ability of non-human objects to act. In other words, an actor/actant is any participant in the network (human or non-human) which has a certain presence and can make a difference to the situation which is being described. In this case, it is preferable to speak of actants rather than actors. In healthcare contexts we can distinguish the actants in Figure 1 as well as a broader set of players. These can include medical instruments, regulators, equipment suppliers (Wickramasinghe, Tatnall, & Goldberg, 2014), and even abstract ideas, such as the concepts of care ethics (van Wynsberghe, 2013), privacy and patient rights, the hippocratic oath and medical standards.

Thus, social robots possess agency - they are actants – and are embedded into networks/ assemblages with human beings, other forms of technology, objects, abstract concepts and ideas. The robot enters coalitions with the various actants in the privacy-healthcare network, establishing translations – one of the key concepts in ANT (see below). A healthcare robot's autonomy, especially with respect to its movements and location, has an impact not only on the patient who the robot serves but also on bystanders. Yet, while the patient may agree to the robot's monitoring and processing of their personal data, bystanders might not. This scenario poses ethical considerations to the extent that a robot's monitoring and actions can impact not only the agency of the individual it serves but also the agency of the individuals surrounding them (Felzmann *et al.*, 2015).

Translation. The term translation describes the process of creating actor-networks as well as the formation of order among the actants. In a translation, the actors in a network influence each other in a process of association (Krieger & Belliger, 2014).[9] In the actor-network of privacy and healthcare robots, translation involves negotiation between additional actants beyond engineers, end-users and the robot itself (Figure 1). Pharmaceutical and healthcare companies, for example, might want to use the robot as an advertising machine, which, based on the patients' own behavioral routines, could promote certain medications or therapies. To do so, such companies would require access to the robot by cooperating with the engineers or by updating the robot's software with a script. Thus, to use the robot as an advertising machine, they would have to enter various coalitions.

Translation is necessary to mediate[10] meaningfully between the various points in the network. Robotics engineers, for example, should think of consumer concerns such as privacy (Calo, 2012; Lutz & Tamò, 2015), security, and job replacement (Eurobarometer 427). They should also implement safeguards in ways accessible by both the end-users and the robots (Lederer, Hong, Dey, & Landay, 2004). This would mean making the privacy and security-related aspects understandable, transparent, and easy to apply for the end-user. For the robot, it would mean using "sustainable" code, algorithms and stable hardware which minimizes privacy hazards and the overall damage potential.

Heterogeneous Networks. A heterogeneous network is one where the interests of the actants are aligned. One can unravel the interests of the actors by interviewing them and tapping into their alliances. With human actants, this is easier than with technological objects or abstract concepts. For technological objects, interviews could include document analysis, *e.g.,* of user manuals (Wickramasinghe *et al.,* 2014), observation of technology-in-use via ethnographic

[9] Latour exemplifies this with the case of a gun and a man. When a tragedy with a firearm occurs, is the human or the gun to blame? Latour would argue that both together (as a hybrid network) lead to killing. "Latour claims that both the man and the gun form a hybrid network which performs according to its own program of action" (Krieger & Belliger, 2014, p. 94). By doing so, he argues against socio-determinism, where technology is seen as neutral and without agency, and against technology determinism, where technology itself acts as a powerful entity and determines how individuals behave.

[10] ANT distinguishes between mediators and intermediaries. Mediators change the state of affairs in a network and are thus important, while intermediaries only transport or pass on other actants without transforming them. Because of their potential of being anthropomorphized and their real-life agency, (social) robots are a prime example of mediators instead of just being an intermediary.

methods, or conversations with the designers and users of the technology. For abstract ideas, this could include the analysis of historical documents and of conversations in action.

In the case of healthcare robots and privacy, we would need to assess the patients' points of view through interviews, assessing whether they value privacy, how they perceive it in relation to other actants (*i.e.*, if they feel it is endangered by doctors or pharmaceutical companies spying on them via a robot), and what they do to protect their privacy. These interviews could be complemented with a document analysis of the robots which utilises user manuals, promotional materials, the internal project transcripts from the engineering team as well as its code and software. They could also be enhanced with an ethnographic analysis of the robot in-action, specifically looking at how privacy is dealt with. Given the recent emergence of healthcare robots, their currently limited adoption and the fact that they are still being developed and in processes of experimentation, carrying out an ANT study about such a research and development project, in the tradition of Latour's laboratory studies, would be a promising approach.

Tokens or Quasi Objects. Tokens are, in essence, the successful interactions of actors in an actor-network - they are being passed through the network. By being passed increasingly through a network, tokens get punctualized (see below), normalized and are progressively taken for granted. By contrast, when tokens are transmitted less frequently or when errors in the transmission of tokens occur (*e. g.*, because a bug interrupts normal routines), punctualization is also decreased and the actor-network faces problems (Zwicker, Seitz, & Wickramasinghe, 2014). In the context of healthcare robots, a successful interaction would entail the successful transmission of health-related information and corresponding actions which would consequently benefit the patient.

Using ANT, social robots can be considered as hybrids, tokens or quasi-objects which Latour (2012) defines as "simultaneously real, discursive and social" (p. 64). The discursive element is particularly interesting since it implies that robots are shaping the discourse around themselves and are shaped by it at the same time. If a majority of people, because of, say, press coverage about a robotic incident (e.g., a Fisher teddy bear or Barbie dolls exposing private

data[11]; or a deadly incident involving a robot at Volkswagen[12]), perceive them as privacy-intruding, dangerous, malign or even creepy, this might feed back on the existing actor-network by inhibiting future purchases of robots or reducing public funding for the research and development of new robots.

Punctualization. Simply put, punctualization is the viewing of a combination of actors as one actor. Punctualization corresponds with black-boxing - it describes how a combination of actants is seen as one actant in a larger network. Thus, punctualization can be considered a form of zooming out, where originally separated actants are seen as one unit. For example, we perceive a mobile phone to be a single entity even though it consists of various components, sub-components and miniscule parts. Similarly, to view healthcare robots as individual actants in an actor-network requires the application of punctualization. This is because such robots are in fact composed of numerous components, ranging from sensory parts such as cameras and microphones, to motorized elements such as arms, legs, or fingers, and even to processing hardware such as computer chips. Punctualiziation is only questioned in moments of crisis and in situations which deviate from the normal functioning of the actor-network. In such instances, de-punctualiziation can occur and the punctualized actant is decomposed into its constituent parts.

In the case of healthcare robots and privacy, robots and their roles in the actor-network might avoid scrutiny as long they function properly and show no signs of violating the privacy of users. However, if a serious privacy breach should occur, the punctualization might be dissolved and de-punctualization might occur. For example, if a healthcare robot should accidentally destroy a meaningful item which belongs to a patient (*e.g.* their diary), this would trigger suspicion as to the proper functioning of the robot. The patient might, for instance, scrutinize the grasping mechanisms in the robot's hands and conclude that they are not properly adjusted. The patient might even attempt to break open the robot's casing to reveal the underlying mechanics – revealing the robot to be a composition of various individual components rather than an entity in its own right. In this sense, privacy breaches can be

[11] https://motherboard.vice.com/read/internet-connected-fisher-price-teddy-bear-left-kids-identities-exposed and http://motherboard.vice.com/read/bugs-in-hello-barbie-could-have-let-hackers-spy-on-kids-chats
[12] http://www.theguardian.com/world/2015/jul/02/robot-kills-worker-at-volkswagen-plant-in-germany

considered triggers for de-punctualization, producing productive, and not just detrimental, outcomes.

Obligatory Passage Point. According to Callon (1986), an obligatory passage point (OPP) is a critical incident where actants in a network converge around an important issue and the survival of the actor-network is at play. The OPP serves as a mediating and transforming element, including its own action program. In the wider context of robots and privacy, an OPP could be a critical incident such as a publically discussed privacy breach. For example, in the instance of the Barbie dolls which listened to the private conversations of children, the dolls were negative perceived by parents. This, in turn, led the Barbie doll producer to rethink the technical functions of their toys. In this sense, the actants of a network have to adjust their interactions in order for the network to remain intact. OPP here necessitates discussions about the technologies integrated in products, the responsibilities of manufactures and the wishes of customers.

In the context of healthcare robots, the agreement needed by various actors to work with specific robots and the creation of data processing standards could be seen as an OPP necessary for establishing the presence of healthcare robots. In addition, legislation or court decisions concerned with how healthcare robots can be employed will impact the network and its actants.

Lessons Learned from ANT with Respect to Privacy

Having now discussed ANT and elaborated on its various concepts within a healthcare context, we now address the lessons learned from the previous section. ANT helps illustrate the far reaching impact of technologies (such as healthcare robots) on society and how the interactions between actants of a network influence the development and adoption of such technologies.

The reciprocal and dynamic nature of ANT illuminates the robotic privacy ecosystem. Indeed, the notion of an ecosystem is perhaps the most fundamental takeaway of any ANT analysis. All actants interact with one another and are co-dependent upon one another. The ecosystem is constantly adapting and re-establishing its “inner balance”. When applied to privacy and robots - or, as stated above, the robotic privacy ecosystem - we must take into

account the delicate balancing needed between various actants' interests. This balancing, in turn, requires a prior assessment of the technologies, concepts and ideas at hand.

Additionally, ANT provides a framework and a common language for facilitating both the description and comparison of networks. For example, it is important to stress that, while considered to be single entities, robots are in fact composed of various units such as cameras, sensors, software and cloud processing operations (see above on punctualization). Therefore, in the context of privacy, each unit might trigger different reactions among actants. Thus, before it is possible to examine the whole actor-network, single units should be analysed.

ANT maps the relationships, interactions and dependencies among actants. It can be used to describe how relationships and responsibilities face alteration once healthcare robots become more present in our homes, nursing facilities, or hospitals. In the words of van Wynsberghe (2013, p. 142): "Beyond the embedding of values and/or norms, once the robot enters a network it will alter the distribution of responsibilities and roles within the network as well as the manner in which the practice takes place." This change is described by the ANT framework - the key term here being "translation". In the context of privacy, the descriptive analysis of relationships is thus key for a better understanding of the issues in question. ANT helps generate the right questions to ask actants in order to better understand the relationships between them.

One such question is the extent of delegation accepted by actants: what factors influence the acceptance of robots as "nurses" or "doctors' assistants"? Linked to that, what data triggers which actions of robots? The more doctors, nurses, or patients delegate tasks to healthcare robots, the more we will be confronted with the question of how robots make decisions. As robots interact progressively more with complex processing systems, gain increased functional abilities and "make a wide range of decisions and apply them on behalf of the user, potentially bypassing active input by the user entirely," it is necessary to identify the underlying mechanisms and the role of user data (Felzmann *et al.*, 2015, p. 282). This includes thinking about the code which robots use and its social implications, such as triggering discrimination or social bonding.

ANT overcomes the limited perspective of technological determinism. It aligns with the socio-technical perspective which argues that technology is not an independent force but must be explained within its political and social context. However, ANT pushes further than the socio-technical view by proposing that the ecosystem as a whole is key. The ecosystem

perspective provides a holistic view of the network and highlights the reciprocal nature of relationships among actants. In that manner, ANT can reconcile two primary paradigms in the context of robots and privacy, indeed also in the context of new technology more generally.

Firstly, ANT stresses that technology itself does not lead to certain outcomes in a deterministic fashion. Thus, it goes beyond the technology-deterministic claims which are all too prevalent in the discourse about robots and privacy (*e.g.*, Carroll, 2015). Robots do not endanger privacy in a linear, predictable fashion. They will not result in the end of privacy and an age of constant surveillance and radical transparency. Instead, they are being embedded in existing and constantly evolving actor-networks of people, interest groups, ideas, social constructions and evolving norms. Thus, they are, to a certain extent, socially shaped and constructed. Secondly, contrary to the diametrically opposite perspective of socio-determinism - or social shaping of technology (Pinch & Bijker, 1984) - these technologies possess agency, interests and embedded values (Brey, 2010). The ways in which they are applied are thus not completely free and arbitrary but constantly negotiated in a diverse network of actants.

Conclusion, Limitation & Future Research

In this contribution, we analyzed the privacy implications of healthcare robots under an ANT lens. We briefly described the technology and suggested that healthcare robots are gaining momentum. That they are here to stay is shown by current demographic trends and higher affordability as well as by increasing tolerance, interest and adoption rates (Rabbitt *et al*., 2015). Increasingly, such robots are networked and Internet-connected, allowing for cloud robotics and the application of big data analysis techniques (van den Berg, 2016). Thus, similar privacy implications as with other current technology developments (IoT, social media, mobile applications etc.) relying on big data analysis and processing occur. However, robots go beyond the informational realm as they possess physical agency and higher autonomy. Focusing on the healthcare area, we then discussed some of the privacy implications of robots. Three types of privacy deemed important in the literature were distinguished: physical privacy, informational privacy and social privacy. For each of these forms, specific challenges and scenarios exist in the healthcare setting. We illustrated a number of such challenges. To describe the privacy implications from a more theoretically substantiated angle we introduced ANT as a suitable approach. After we had outlined the basic assumptions and modus operandi of ANT, we proceeded to describe the healthcare robot privacy ecosystem by applying key terminology of

ANT to the issue. Such key concepts include, among others, actants (robots have agency and ingrained programs), translation (robots and other actants in the network enter associations to coordinate themselves), punctualization (the fact that a robot is perceived as an entity on its own instead of a sum of individual parts) and obligatory passage points (critical events for the survival of the actor-network). Each of these concepts illustrated another important aspect in the healthcare robot privacy ecosystem, thus allowing us to describe the phenomenon more holistically and in a more nuanced way. Finally, we summarized the key learnings from the ANT analysis: seeing privacy and healthcare robots as a complex issue where technology-determinism and social determinism clash and must be reconciled; appreciating the role of actants one traditionally does not think of (pharma companies, historical reasoning and ideas, semiotic elements—such as news stories or instruction manuals—, code, algorithms, physical design features etc.); inspiring efforts how to investigate the topic empirically (with case studies and broad ethnographic research).

Despite its contributions, ANT has been criticized by the research community to be not enough of a scientific method. Some critics argue that the ANT analysis leads to no objective insights and does not offer insights on how to improve the status quo (Boltanski & Chiapello, 2005). Others are skeptical of the agency of things (Schaffer, 1991).

Future research will have to address the concrete question of how to deal with perceived and experienced privacy issues. Van den Berg (2016), for instance, brought forward a controversial idea that all privacy issues in the context of robots will disappear if robots are simply not connected to the Internet. The argument here is that only because of the connectivity and cloud processing of data privacy breaches occur. Van den Berg (2016) states:

> "*The idea that robots register us, and store data about us in our homes, is not a reason for concern, let alone for privacy or security concerns. After all, when other human beings come into our homes they, too, 'register' and 'store' information about us using their 'sensing devices'.*" (p. 7).

According to her, the reason for security and privacy concerns with social robots is their connection to the Internet and, in some cases, the cloud, with the potential to provide access to sensitive information collected inside the home (p. 8). Such measures of taking critical infrastructure off the Internet have been taken, for instance, for nuclear power plants or water facilities. Van den Berg's argument, while interesting, is in our opinion impracticable though as cloud robotics is a breakthrough technology in robotics and will highly support the

deployment of robots. Furthermore, it goes against the developments we see with smart devices (the Internet of Things as a key word here).

Nonetheless, we agree with van den Berg's (2016) plea to think about privacy before designing robots. As we have argued in a previous paper, thinking about privacy and ethical issues raised by the employment of robots requires specialists who understand not only the technology behind robots but also the legal frameworks that need to be taken into account when developing (social) robots (Lutz & Tamò, 2015).

References

Ackerman, E. (2015). Robots Might Be the Necessary Future of Urban Pet Ownership, in: http://spectrum.ieee.org/automaton/robotics/home-robots/robots-might-be-the-necessary-future-of-urban-pet-ownership (posted in May 2015)

Aeschlimann, L., Harasgama, R., Kehr, F., Lutz, Ch., Milanova, V., Müller, S., Tamò, A., Strathoff, P., (2015). Re-Setting the Stage for Privacy: A Multi-Layered Privacy Interaction Framework and Its Application. In Brändli et al. (Eds.), *Mensch und Maschine - Symbiose oder Parasitismus?* (pp.1-41). Bern: Stämpfli.

Alaiad, A., & Zhou, L. (2014). The determinants of home healthcare robots adoption: An empirical investigation. *International Journal of Medical Informatics, 83*(11), 825-840.

Altman, I. (1975). *The environment and social behavior: privacy, personal space, territory, crowding*. Monterey, CA: Brooks/Cole.

Bekey, G. (2012). Current Trends in Robotics: Technology and Ethics. In P. Lin, G. Bekey, & K. Abney (Eds.), *Robot Ethics: The Ethical and Social Implications of Robotics* (1st ed., pp. 17-34). Cambridge, MA: MIT Press.

Boltanski, L., & Chiapello, E. (2005). *The new spirit of capitalism*. London, UK: Verso [First French edition: *Le nouvel esprit du capitalisme*. Paris, Gallimard 1999]

Breazeal, C. (2003). Toward sociable robots. *Robotics and autonomous systems, 42*(3), 167-175.

Brey, P. (2010). Values in technology and disclosive computer ethics. In. L. Floridi (Ed.), *The Cambridge Handbook of Information and Computer Ethics* (pp. 41-58). Cambridge, UK: Cambridge University Press, Cambridge (UK), 41–58.

Burgoon, J. K. (1982). Privacy and communication. In M. Burgoon (Ed.), *Communication Yearbook 6* (pp. 206-249). Beverly Hills, CA: Sage.

Callon, M. (1986). Elements of a sociology of translation: Domestication of the Scallops and the Fishermen of St Brieuc Bay. In J. Law (Ed.), *Power, Action and Belief: A New Sociology of Knowledge?* (pp. 196-233). London, UK: Routledge.

Calo, R. (2012). Robots and Privacy. In P. Lin, G. Bekey, & K. Abney (Eds.), *Robot Ethics: The Ethical and Social Implications of Robotics* (1st ed., pp. 187-202). Cambridge, MA: MIT Press.

Calo, R. (2015). Robotics and the Lessons of Cyberlaw. *California Law Review, 103*, 2014-08.

Carroll, R. (2015). Goodbye privacy, hello 'Alexa': Amazon Echo, the home robot who hears it all. *The Guardian*, 21 November. Retrieved from http://www.theguardian.com/technology/2015/nov/21/amazon-echo-alexa-home-robot-privacy-cloud

Clarke, R., & Moses, L. B. (2014). The regulation of civilian drones' impacts on public safety. *Computer Law & Security Review, 30*(3), 263-285.

Darling, K. (2012). Extending legal rights to social robots. *SSRN Electronic Journal*. Retrieved from http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2044797

Darling, K. (2016), Extending legal protection to social robots: The effects of anthropomorphism, empathy, and violent behavior towards robotic objects. In R. Calo, M. Froomkin & I. Kerr. (Eds.), *Robot Law* (pp. 213-234). Northampton, MA: Edward Elgar Publishing.

Duffy, B. R. (2003). Anthropomorphism and the social robot. *Robotics and autonomous systems, 42*(3), 177-190.

Eurobarometer 427 (2015). Autonomous Systems. Report retrieved from http://ec.europa.eu/public_opinion/archives/ebs/ebs_427_en.pdf

Felzmann, H., Beyan, T., Ryan, M., & Beyan, O. (2015). Implementing an ethical approach to big data analytics in assistive robotics for elderly with dementia. In *Proceedings of the 2010 ACM ETHICOMP Conference* (pp. 280-286), Leicester, 7-9 September.

Gonçalves, F. A., & Figueiredo, J. (2014). Disturbing Practices in Engineering Design Projects. In A. Tatnall (Ed.), *Technological Advancements and the Impact of Actor-Network-Theory* (pp. 238-251). Hershey, PA: IGI Global.

Gupta, S. K. (2015). Six Recent Trends in Robotics and Their Implications. *IEEE Spectrum*, 8 September.

Krieger, D. & Belliger, A. (2014). *Interpreting Networks: Hermeneutics, Actor-Network Theory & New Media.* Bielefeld: Transcript Verlag.

Latour, B. (1987). *Science in Action: How to Follow Scientists and Engineers Through Society*. Milton Keynes: Open University Press.

Latour, B. (1994). On technical mediation—philosophy, sociology, genealogy, in: Common Knowledge 3(2), pp. 29-64.

Latour, B. (2005). *Reassembling the Social. An Introduction to Actor-Network-Theory*. Oxford: Oxfrod University Press.

Lederer, S., Hong, J. I., Dey, A. K., & Landay, J. A. (2004). Personal privacy through understanding and action: Five pitfalls for designers. *Personal and Ubiquitous Computing, 8*(6), 440-454.

Lin, P. (2012). Introduction to Robot Ethics. In P. Lin, G. Bekey, & K. Abney (Eds.), *Robot Ethics: The Ethical and Social Implications of Robotics* (1st ed., pp. 3-16). Cambridge, MA: MIT Press.

Lutz, C., & Tamò, A. (2015). RoboCode-Ethicists: Privacy-friendly robots, an ethical responsibility of engineers? In *Proceedings of the 2015 ACM SIGCOMM Workshop on Ethics in Networked Systems Research* (pp. 27-28), London, August 21.

Mann, J., MacDonald, B., Xingyan Li, H., & Broadbent, E. (2015). People respond better to robots than computer tablets delivering healthcare instructions. *Computers in Human Behavior, 43*(2), 112–117.

Margulis, S. T. (2011). Three theories of privacy: An overview. In S. Trepte, & L. Reinecke (Eds.), *Privacy Online* (pp. 9-17). Heidelberg/Berlin, DE: Springer.

Muhammad, I., & Wickramasinghe, N. (2014). How an Actor Network Theory (ANT) Analysis Can Help Us to Understand the Personally Controlled Electronic Health Record (PCEHR)

in Australia. In A. Tatnall (Ed.), *Technological Advancements and the Impact of Actor-Network-Theory* (pp. 15-34). Hershey, PA: IGI Global.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review, 79*, 119-157.

Petronio, S. (2002). *Boundaries of privacy: dialectics of disclosure*. Albany, NY: State University of New York Press.

PEW Research Center (2014). Global Opposition to U.S. Surveillance and Drones, but Limited Harm to America's Image. Study published in June 2014. Retrieved from http://www.pewglobal.org/2014/07/14/global-opposition-to-u-s-surveillance-and-drones-but-limited-harm-to-americas-image/ (cited: PEW 2014)

Pinch, T. J., & Bijker, W. E. (1984). The social construction of facts and artefacts: Or how the sociology of science and the sociology of technology might benefit each other. *Social Studies of Science, 14*(3), 399-441.

Rabbitt, S. M., Kazdin, A. E., & Hong, J. H. (2015). Acceptability of robot-assisted therapy for disruptive behavior problems in children. *Archives of Scientific Psychology, 3*(1), 101. Retrieved from http://psycnet.apa.org/journals/arc/3/1/101.pdf&uid=2015-34826-001&db=PA

Schaffer, S. (1991). The eighteenth Brumaire of Bruno Latour. *Studies in History and Philosophy of Science, 22*, 174-192.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS Quarterly, 35*(4), 989-1016.

Syrdal, D. S., Walters, M. L., Otero, N., Koay, K. L., & Dautenhahn, K. (2007). "He knows when you are sleeping" – Privacy and the personal robot companion. In *Proceedings of the 2007 AAAI Workshop Human Implications of Human–Robot Interaction*, (pp. 28-33), Washington DC, 9-11 March.

Trepte, S., & Reinecke, L. (2011). The social web as a shelter for privacy and authentic living. In S. Trepte, & L. Reinecke (Eds.), *Privacy Online* (pp. 61-74). Heidelberg/Berlin, DE: Springer.

Turkle, S. (2011). Authenticity in the age of digital companions. In M. Anderson & S. L. Anderson (Eds.), *Machine Ethics* (1st ed., pp. 62–76). Cambridge, United Kingdom: Cambridge University Press.

Van den Berg, B. (2016). Mind the Air Gap. In S. Gutwirth, R. Leenes, P. De Hert (Eds.), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection* (pp. 1-24). Dordrecht, NL: Springer Netherlands.

Van Wynsberghe, A. (2013). Designing robots for care: Care centered value-sensitive design. *Science and Engineering Ethics, 19*(2), 407-433.

Warren, S., & Brandeis, L. (1890). The right to privacy. *Harvard Law Review, IV*(5),193-220

Westin, A. F. (1967). *Privacy and freedom*. New York, NY: Atheneum.

Wickramasinghe, N., Tatnall, A., & Goldberg, S. (2014). How the Rich Lens of ANT Can Help us to Understand the Advantages of Mobile Solutions. In A. Tatnall (Ed.), *Technological Advancements and the Impact of Actor-Network-Theory* (pp. 87-99). Hershey, PA: IGI Global.

Zwicker, M., Seitz, J., & Wickramasinghe, N. (2014). E-Health in Australia and Germany. In A. Tatnall (Ed.), Technological Advancements and the Impact of Actor-Network-Theory (pp. 145-160). Hershey, PA: IGI Global.