USING ACTOR-NETWORK THEORY TO MINIMIZE RISK IN CONSUMER ROBOTICS

A Research Paper submitted to the Department of Engineering and Society
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Engineering

By

Kellan Delaney

March 28, 2022

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

ADVISOR
Catherine D. Baritaud, Department of Engineering and Society

GROWTH OF CONSUMER ROBOTICS

The consumer robotics market is growing rapidly, with revenues of 4.122 billion USD in 2019 to an expected 32.8 billion USD in 2027 (GMI Research, 2021). Especially during the COVID-19 pandemic as people spend more time inside their homes, spending has shifted more toward inside the home expenses than outside the home, including on consumer robots, leading to a 4.3% increase in revenues from pre-pandemic expectations (Edwards, 2021). For this paper, a consumer robot is defined as a device with onboard computing power that helps people with tasks by interacting with the world around it in some physical manner. These machines help people in their daily lives in many ways including cleaning, household care, healthcare, entertainment, education, or just keeping company (Maynard, 2019). Some examples include the robotic vacuum Roomba (iRobot, n.d.), the programmable humanoid robot NAO (SoftBank Robotics, n.d.), and robot dog Aibo (Sony, n.d.).

With this upshift in prevalence, it is also important to take note of this technology's potential impacts on society. The world is no stranger to connected devices and the Internet of Things (IoT). IoT refers the system of interconnected devices that can communicate with each other and share resources over a network. With many robotic devices being introduced, a physical interface is being put on the computing power of the internet, creating the Internet of Robotic Things (Matthews, 2019). This could introduce many new ways to collect data on people, which has historically been a very controversial topic. More commonplace consumer robots also means that people could be physically harmed by their devices. Even if unintentional, the fact that there are moving parts that are meant to interact with a human means that something could go wrong and cause the robot to hurt its user. This STS research paper seeks to explore the safety and security concerns associated with the advancement of consumer robotics and answer

the question: How can engineers design consumer robotics with minimal security and privacy risks to their users? Actor-Network Theory (ANT), first described by Michel Callon, Bruno Latour, and John Law in the late 1980s and 1990s, is a very helpful framework which can be used to explore relationships between both humans and non-humans and to assist in answering this question (Cressman, D).

Tightly coupled to the STS topic is the technical project, in which the capstone team aimed to design and build a consumer robot in the form of a semi-autonomous robot that can play Connect 4 against a human player. Physical safety was more emphasized in this project. The capstone team consisted of the author of this paper, Kellan Delaney, as well as Jared Tyranski and Roman Kaker, all of whom are Electrical and Computer Engineering undergraduate students at the University of Virginia. This project was conducted under the advisement of Electrical and Computer Engineering Professor Harry C. Powell Jr.

PRIVACY AND SECURITY VULNERABILITIES FROM CONSUMER ROBOTS

Introducing consumer robots into society can introduce a variety of risks to their users. Dimov (2015), an expert in internet law, identifies five primary types of provacy and security risks associated with increasing use of household robots, which in this paper are considered to be synonymous with consumer robots. These risks are described in Figure 1 on the next page. If during the design process of a consumer robot, engineers only strive to achieve their desired functionality, then these risks are turned into explicit vulnerabilities that could cause harm to the user. All of the risks mentioned have one important factor in common. They all involve a person with malicious intent gaining control of the robot and exploiting its vulnerabilities in pursuit of

their own interest. These individuals could collect sensitive data or force the robot to behave in ways that could physically or mentally harm a user.

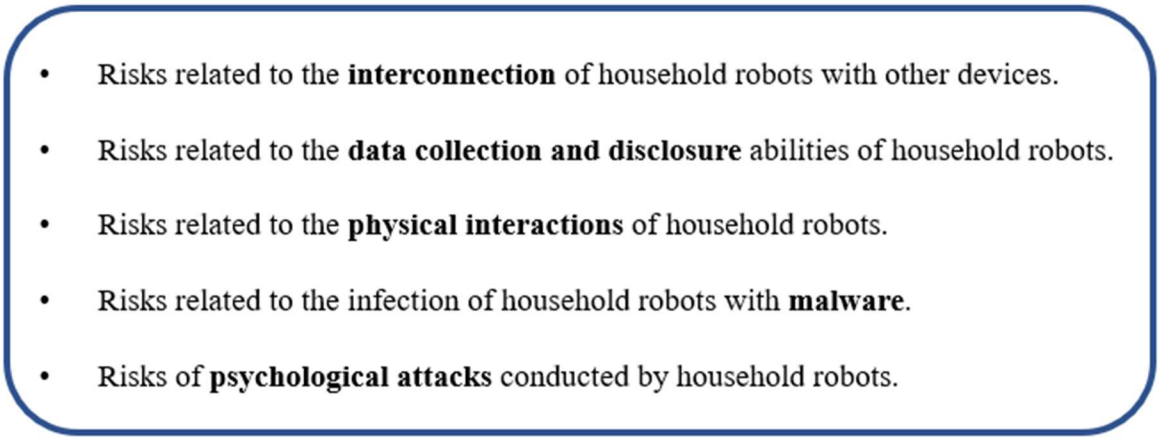

Figure 1: Risks Related to Consumer Robots. These are the primary risks associated with the increasing use of consumer robots. (Created by Delaney (2022)).

Physical safety is perhaps the most critical and certainly the most obvious of safety criteria in the design of robots. Exposed electronics with high voltages or currents and moving parts have the potential to physically harm a user if they are not designed with safety in mind. Preventing mental harm caused by robots on the other hand is something much more abstract. When people use robots, they may form an emotional bond with their device. This is especially true in the case of social or caretaking robots. This concept is explored in depth in the film, *Robot & Frank*, in which retired criminal Frank becomes friends with his caretaker robot through shared experiences (Schreier, 2012). The actions of a robot have the potential to psychologically manipulate or harm the user if controlled by someone with malicious intent.

The ever-growing Internet of Things is an easy entryway for consumer robotics to enter many households (Petrara, 2019). If a robot can use smart home devices that are already in a home, consumers will be incentivized to buy and use it. While this is a great way to take advantage of existing technology, it also presents the first risk described, associated with the

interconnection of consumer robots with other devices. If everything is connected to a single network, it is much easier for a hacker to hijack the system and collect data or control a device. The simplest solution to this problem is to have the robot completely isolated from any networks. However, then the robot cannot ultilize any data from other devices or processing power on the Internet. There are likely solutions that allow the robot to have a more secure connection through things like encryption and firewalls, but that is beyond the scope of this paper.

The issue of privacy is also a concern for many people, especially in the United States (Auxier et al., 2019). With consumer robots, another opportunity to have personal information collected and tracked is introduced. Many current internet based products and services track user data in order to improve user experience. However, according to a study done at the University of South Wales, most of these devices are extremely insecure and their data can be accessed with fairly simple techniques (Sivaraman et al., 2018). This practice is likely to also occur in consumer robots where data collection could offer the same potential user experience benefits while neglecting security features can cut down on costs. A common solution to this ethical dilemma is to offload the decision making to the user by allowing them to opt-in to the data tracking service. Then it is up to the user to decide whether or not they want their information tracked and shared.

Most existing standards regarding the design of robotics are specifically for physical safety of industrical robots. Industrial robots are mostly used for manufacturing and are deployed in factories with little intention for human-robot interaction. It is good that they have safety standards, but those standards do not apply for consumer robots which are meant to interact with humans. This is concerning given the rising number of daily interactions with consumer robots. In addition, current standards do not resolve the risks that were presented earlier beyond the

physical, including mental health and cybersecurity issues, a discrepancy that should be addressed before consumer robots become any more widespread (Martinetti et al., 2021).

ACTOR-NETWORK THEORY CLARIFIES VULNERABILITIES IN CONSUMER ROBOTICS

In most engineering design processes, among the first steps is defining the technical requirements for the project. Engineers then focus on fulfilling those technical requirements in order to complete the project. When naively performed, this practice can lead to tunnel vision for the engineers, who are only considering technical requirements and are neglecting to consider the social implications of their desings. In consumer robotics, this neglect leads to vulnerabilities related to the safety, security, and privacy issues previously defined. However, focusing too solely on the social and human aspects of a project can lead to diminished quality in the technical work. Therefore, there must be some method with which to analyze both the non-human and human aspects of a project. Venturini (2010), a researcher at the CNRS Centre for Internet and Society, says that actor-networks are what must be analyzed in order to truly understand a system. Engineers can use this tool of actor-network analysis to examine both the non-human and human actants in a system and the network of relationships between them. By doing this, engineers can more fully understand how their design will integrate into society and any implications associated with that integration.

Even knowing the idea to consider the relationships between human and non-human actants, it can still be difficult to conceptualize exactly what role a particular engineering design will play in an actor-network. Latour (1992) describes a method to determine a non-human's role in an actor-network in which that non-human is replaced with another non-human or a human

that behaves in its place (p. 229). In this way, consumer robots can be viewed as humans performing the same roles, making the relationships in the network much more clear. Roombas are now domestic cleaners who vacuum the floors and learn about a floor plan. A robot that reminds the elderly to take medicine is now a nurse who knows all about their patients medical needs. A personal robot assistant is now a butler who is intimately familiar with your daily habits.

Turning consumer robots into human actors also demonstrates more simply how they can be exploited by hackers. The domestic cleaner who knows the floor plan of a house can be interrogated and have that information extracted to be used for planning a burglary. The nurse can expose sensitive medical information which could be used to harm the patient. The butler can be tricked into telling a criminal when a house will be empty. These are all extreme examples, but demonstrate how useful the process of turning a non-human actor into a human actor can be.

Actor-Network Theory also highlights the main stakeholders of the development of consumer robotics, mainly being users who are directly affected by the product, non-users who are indirectly affected by the product, designers who create the product, and hackers who attempt to exploit the product. Big ideas that should also be included in the network are privacy, and security. Figure 2 below illustrates the actor-network system associated with consumer robots designed by naïve engineers who are not engaging in actor-network analysis. Note that the engineers do not have a direct connection to privacy and security, because they are only focusing on the technical aspects of their design of the consumer robot. They do have an indirect influence on privacy and security through however they design the robot.

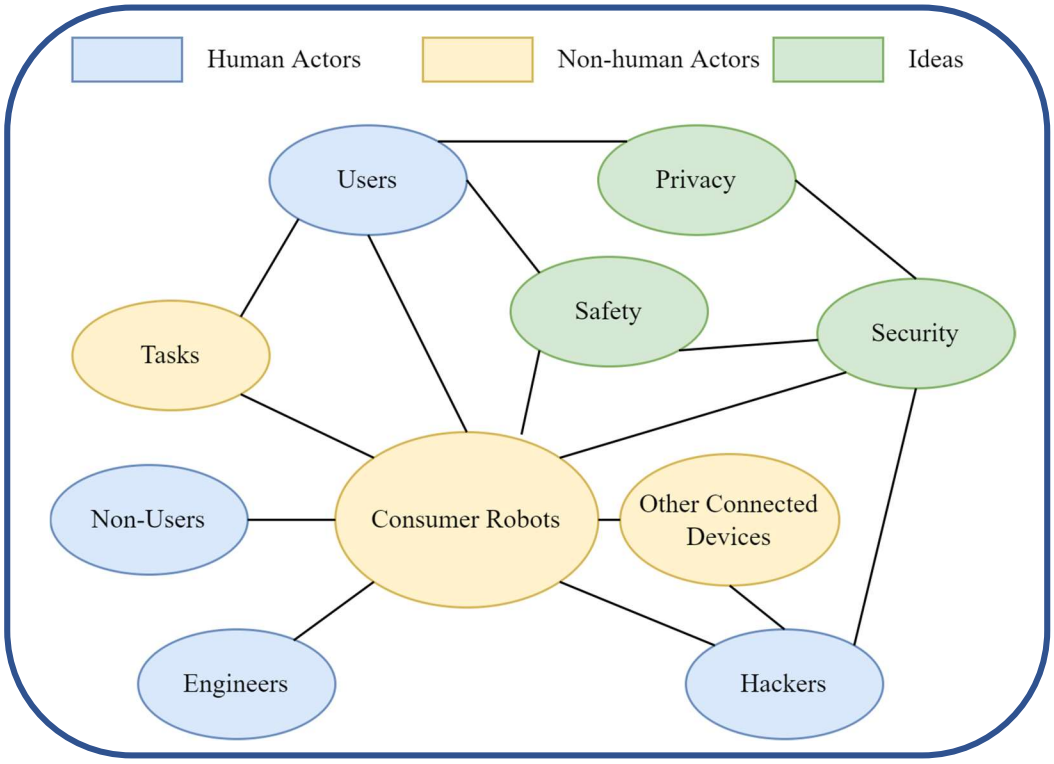

Figure 2: Preliminary Actor Network Model. This model shows the relationships between human actants, non-human actants, and the ideas surround them in consumer robot design. (Created by Delaney (2022)).

ENGINEERING MORE SECURE CONSUMER ROBOTS WITH ACTOR-NETWORK ANALYSIS

In order to design more secure consumer robots, engineers should adopt this style of actor-network thinking. First, they must consider the actor-network specific to their robot and their robot's role in that actor-network, which could be done by considering how a human actor would act in its place. Then, they must think critically about how their product could be exploited and how that exploitation could affect the users. It can be helpful to consider the worst possible case, where they should consider every part of their design a possible vulnerability. This process will help engineers more easily identify vulnerabilities in their design and correct them. In addition, it forces engineers to be more conscientious about safety, security, and privacy in their designs for consumer robots, therefore protecting the users.

When engineers are more considerate of users and the factors in their designs that affect them, the connection between the engineers, the users, and those factors becomes stronger in the actor-network. Figure 3 on the next page illustrates the new actor-network system with stronger connections between engineers, users, and the factors affecting the users. In contrast to Figure 2, the engineers in this system are having a direct influence on safety, security, privacy, and the users.

Actor-network analysis should also be done at every stage of the design process as more knowledge about the product gets acquired. That way, as the design evolves, it is much more flexible and receptive to changes in understanding of actants and their relationships. In general, this is true of any method of social consideration during the engineering design process. It should not be a single step isolated at the beginning or end of design. It should be revisited frequently.

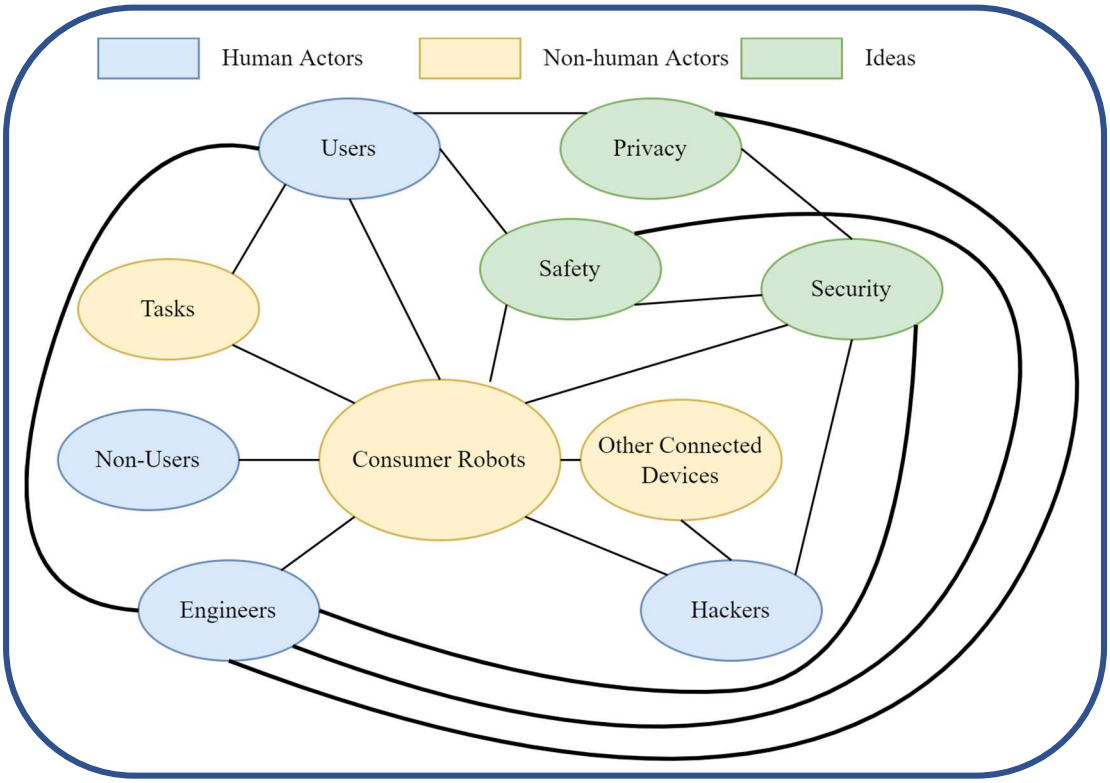

Figure 3: Improved Actor Network Model. This improved model shows how engineers can have a direct influence on safety, security, privacy, and users when using actor-network thinking. (Created by Delaney (2022)).

APPLIED EXAMPLE WITH AIBO

To explore this process further, the example of Sony's robot dog Aibo (Sony, n.d.) will be used. Its actor-network consists of many of the same features as a general consumer robot, with the addition of the cloud service as a non-human actant. Its intended role in the actor-network is to perform many of the same tasks that a real dog would do, with some additional features. Primarily, it provides companionship to its users by playing with them, learning their faces, and having unique interactions that collectively shape its identity. Regarding additional features, it connects to a cloud service on the internet, where it uploads recordings of everything that it experiences. This is meant to allow users to go back and view Aibo's memories. One unintended role that it is performing is potentially providing a new route which hackers can use to monitor people.

To prevent a worst case scenario, every possible vulnerability of Aibo must be explored and protected against. The main potential vulnerability in Aibo is its connection to the internet. If it is connected to the internet, then it is also connected to a shared network to which other devices are likely connected. Each connected device on the network is a potential access point, which a hacker can use to monitor the network. If a hacker gains access to the network, they can monitor the packets leaving Aibo to upload to the cloud service. If unprotected, this could give a hacker a live video feed of everything that Aibo is seeing. This access is a serious invasion of privacy to the users and should be protected against. Another potential vulnerability is at the cloud service. If the database containing the recordings itself is unprotected, then a hacker could gain access to that via the internet, constituting another serious invasion of privacy. The cloud service is also where an AI is running to let Aibo learn. A hacker could block messages from the cloud service to Aibo and send their own message to Aibo, influencing its behavior. Given

Aibo's purpose as a companion robot, affecting its behavior could have serious emotional effects on the user. Figure 4 on the next page shows the actor-network model for Aibo. Note that the cloud service also affects security, which is a unique feature to this actor-network.

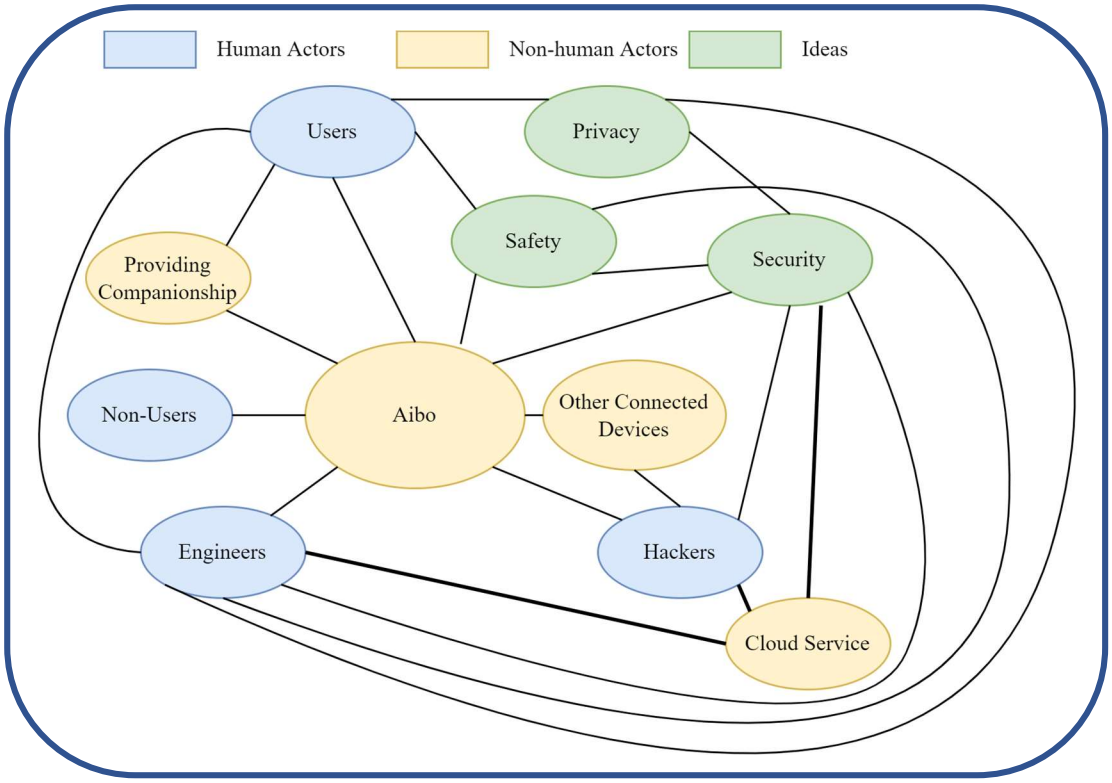

Figure 4: Aibo Actor-Network Model: This model shows the unique relationships surrounding the Aibo robot dog. (Created by Delaney (2022)).

ADAPTABILITY OF ACTOR-NETWORK ANALYSIS FOR FUTURE DESIGNS

Looking to the future, consumer robots will likely become more common every year and soon will become a part of many people's everyday lives. With innovation, though, comes new problems which need solutions. It can be difficult to anticipate exactly what problems might occur, so a more generally applicable solution must be identified in order to ensure user risks are minimized. With the lack of current standards to ensure consumer robots do not present a risk to their users, using actor-network theory can help engineers who are designing future consumer robots to anticipate consequences of their design and minimize risk to their users. This

suggestion does not provide specific technical directions to take in combating safety, security, and privacy risks. However, it is adaptable to all situations and all types of consumer robots. There is no general solution to risks in consumer robotics, but with careful use of ANT analysis, engineers can identify the best solution for their specific device.

REFERENCES

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019, November 15). *Americans and privacy: Concerned, confused and feeling lack of control over their personal information*. Pew Research Center. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Cressman, D. (2009, April). *A brief overview of actor-network theory: Punctualization, heterogenous engineering & translation*. Centre for Policy Research on Science & Technology, School of Communication, Simon Fraser University.

Delaney, K. (2022). *Aibo Actor-Network Model*. [Figure 4]. *STS Research Paper*: Using actor network theory to minimize risk in consumer robotics (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Delaney, K. (2022). *Improved Actor-Network Model*. [Figure 3]. *STS Research Paper*: Using actor network theory to minimize risk in consumer robotics (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Delaney, K. (2022). *Preliminary Actor-Network Model*. [Figure 2]. *STS Research Paper*: Using actor network theory to minimize risk in consumer robotics (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Delaney, K. (2022). *Risks Related to Consumer Robots*. [Figure 1]. *STS Research Paper*: Using actor network theory to minimize risk in consumer robotics (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Dimov, D. (2015, October 16). *Privacy risks of household robots: 5 security risks and 10 steps to protect yourself*. Infosec. https://resources.infosecinstitute.com/topic/privacy-risks-of-household-robots-5-security-risks-and-10-steps-to-protect-yourself/

Edwards, D. (2021, February 16). *Pandemic lockdowns boost consumer robotics market to $10 billion in 2020 revenues*. Robotics and Automation News. https://roboticsandautomationnews.com/2021/02/16/pandemic-lockdowns-boostconsumer-robotics-market-to-10-billion-in-2020-revenues/40492/

GMI Research. (2021, May 20). *Consumer robotics market research reports, opportunities & forecast 2020-2027*. https://www.gmiresearch.com/report/global-consumer-robotics-market/

iRobot. (n.d.). *Roomba robot vacuum cleaners*. https://www.irobot.com/roomba

Latour, B. (1992). Where are the missing masses? The sociology of a few mundane artifacts. In Bijker, W.E. & Law, J. (Eds.), *Shaping technology/building society: Studies in sociotechnical change* (pp. 225-258). MIT Press.

Martinetti, A., Chemweno, P. K., Nizamis, K., Fosch-Villaronga, E. (2021, July 27). Redefining safety in light of human-robot interaction: A critical review of current standards and regulations. *Frontiers in Chemical Engineering*, *3*. https://doi.org/hhvq

Matthews, K. (2019, June 19). *The internet of robotic things: how IOT and robotics tech are evolving together*. EETimes. https://iot.eetimes.com/the-internet-of-robotic-things-how-iot-and-robotics-tech-are-evolving-together/

Maynard, N. (2019, August 09). *The evolution of consumer robotics*. Juniper Research. https://www.juniperresearch.com/resources/analystxpress/august-2019/the-evolution-of-consumer-robotics

Petrara, D. (2019, August 22). *Consumer robotics is a market in transition; smart home will be at the heart of the change*. Business Wire. https://www.businesswire.com/news/home/20190822005033/en/Consumer-Robotics-is-a-Market-in-Transition-Smart-Home-Will-be-at-the-Heart-of-the-Change

Schreier, J. (Director). (2012). *Robot & Frank* [Film]. Samuel Goldwyn Films.

Sivaraman, V., Gharakheili, H. H., Fernandes, C., Clark, N., & Karliychuk, T. (2018, June 04). Smart IOT devices in the home: Security and privacy implications. *IEEE Technology and Society Magazine*, *37*(2), 71-79. https://doi.org/gnc73x

SoftBank Robotics. (n.d.). *NAO the humanoid and programmable robot*. https://www.softbankrobotics.com/emea/en/nao

Sony. (n.d.). *aibo*. https://us.aibo.com/

Venturini, T. (2009). Diving in magma: How to explore controversies with actor-network theory. *Public Understanding of Science*, 19(3), 258-273.