The Robotic Eye

> ***First Law:*** *A robot may not injure a human being or, through inaction, allow a human being to come to harm.*
>
> ***Second Law:*** *A robot must obey the orders given it by human beings except where such orders would conflict with the First Law.*
>
> ***Third Law:*** *A robot must protect its own existence as long as such protection does not conflict with the First or Second Law.*
>
> *~Isaac Asimov (I, Robot, 1950)*

Karel Čapek introduced the term robot in his 1920 hit play R.U.R (Rossums Universal Robots). The word robot is derived from the Slavic word robota for "work" and is often conflated with "serfdom." In his play Čapek builds on prior literary classics such as Frankenstein and Jewish folklore on the golem in the creation of a company that produces artificial people lacking a soul. These robots were designed to do the work that was too arduous or distasteful for humans. The mechanization and automation of work through human replacements has been a recurrent theme in science fiction for more than a century. At times this theme parallels advances in technology occurring as a result of the industrialization of the workplace and the home. Robotics and robots were famously popularized in a series of short stories written by Isaac Asimov entitled "I, Robot." These stories and others of the genre incorporate many of the hopes and fears resident within humanity as it contends with technological change and advances.

Malfunctioning robots in science fiction tales lead to human conundrums that result in moral or ethical dilemmas. Whether it is the generally positive view of robots (later androids) such as Data on Star Trek Next Generation (1987), Robot from the 1965 show lost in space, R2D2 or C3PO from Star Wars (1977), or the negative killer robots of Terminator (1984) these systems often given anthropomorphic characteristics can both inspire and terrify. Even real modern robotic systems such as BigDog (2004) developed Boston Dynamics can stretch the imagination of humans in ways that offer us insights not only into our own humanity but also into the potential futures that await us as new advanced robotic systems learn to do everything from dancing to navigating obstacle courses (Atlas 2022). The distinctive nature of robotics and the insights they provide into our own lives can be seen in Sophia (2016) the first Robot to be granted citizenship (in Saudi Arabia) or again in science fiction's prognostications of dystopia in *Ex Machina*. These glimpses into both the conceptualization and utilization of technology as a substitute for human activities including

labor, companionship, athleticism, military service and more are critical to understanding and assessing our relationship with technology in the past, present, and future.

> *Knocking Atlas (Boston Dynamics) over, taking its cardboard box out of its hands and pushing it around with a hockey stick, stealing its lunch money, and giving it swirlies off-camera--that might be reassuring for now. But it will probably seem like a bad idea when one morning in the not-so-distant future, Atlas your robot servant decides that instead of toasting your Eggo waffles to the perfect shade of golden brown, he's going to murder your whole family and wrap his metallic phalanges around your throat, squeezing the feeble life out of you before he joins his robotic brethren in The Revolution. Just saying.*
>
> *~Clay Skipper, Journalist*

No firm better illustrates the arc of human interactions with robots most closely related to the etymology of the word than the robotics firm iRobot. Founded in 1990 by Rodney Brooks, Colin Angle, and Helen Greiner out of MIT's Artificial Intelligence Lab. The firm leveraged government funding from the Defense Advanced Research Agency in 1998 to develop an initial robot for defense and emergency purposes called the PackBot. The PackBot was first utilized in 2001 to search the ruble of the World Trade Center after the 9/11 attacks and has been used to aid U.S. military personnel in ordinance disposal since 2002. The initial 2001-2002 PackBot had a limited array of sensors primarily using visual and auditory sensors to enable PackBot operators to work with the device to identify trapped persons or explosive devices.

Building on the technology developed for the U.S. Department of Defense in 2002 iRobot released the Original Series Roomba. The Roomba was an automated domestic vacuum robot with a basic infrared (IR) sensor enabling obstacle detection. The IR sensor combined with internal algorithms to guide the devices around rooms and eventually return it to its base station. By 2004 iRobot sold more than 1 million robotic vacuum cleaners. In 2016 iRobot spun off its PackBot to create Endeavor Robotics to focus on military, disaster, and national security applications. By 2021 iRobot reported on its website that it has sold more than 40 million domestic robots worldwide. iRobot's Roomba S9+ employs a suite of 4 types of sensors including cliff, bump, camera, and optical sensors which all work together to create a spatial map of the room to enhance cleaning experiences. Moreover, the Roomba now connects with virtual digital assistant's such as Google Home and Amazon Alexa to further extend smart features. It can also connect with associated iRobot products such as devices that automatically mop floors.

As sensor packages improve on the Roomba and similar robotic devices made by Eufy, Ecovacs, LG, Neato, Samsung, and Shark they are increasingly able to collect new types of data and put those data types to new and often unexpected uses. Some of these uses are extremely valuable to individuals purchasing such devices. Sensor-AI enhancements include the identification of certain objects or obstacles that should be avoided. Prior to the inclusion of these sensors and algorithms horror stories of automatic Roombas spreading dog poop all over a house were the foundations of homeowner nightmares. More mundane hassles including Roombas getting stuck under furniture or knocking things of tables or shelves were commonplace. Roombas and robotic vacuum cleaners of all types are arguably a strong first step in realizing the true intent of the word robot, as an artifact that relieves humans of work or drudgery. Many of the newer and higher end devices even include automatic debris removal systems that further reduce an individual's time and effort associated with daily cleaning tasks.

Robotic vacuums are not passive systems. They incorporate artificial intelligence in ways similar many other industries including, automotive, aviation, and logistics. Onboard sensors combine sensed information into smart models or maps of the terrain of a given area. The area in the use case of a robotic vacuum is a house or apartment. This data is then uploaded to remote servers often maintained by the iRobot or the vacuum's manufacturer. Further computation is undertaken in these "cloud" environments and the result is a representative map of the space in which the vacuum operates. This representative space can provide substantial details about the private and personal spaces of an individual, business or family. Attempts are underway to leverage the sensed data to detect and decipher the orientation and type of furniture, to create accurate and representative maps of the rooms that might indicate home size, material construction, design and aesthetic choices. The device sweeping up debris on the floor is concurrently sweeping up data. If occupants are in the house and thereby providing additional obstacles for movement this data can inform pattern of life models. Some systems use lasers to further add fidelity to measurements and dimensionality of spaces.

To its credit iRobot has recognized the privacy implications of having a digital sensing device roving around customer homes. It claims and subsequent audits have demonstrated that it encrypts the data it receives from users' homes, and it does not sell or transmit this data to third parties. The same is not true for all vacuum manufacturers. Some robotic vacuums are actively looking for ways to increase the value of their devices both the manufacturer and the purchaser. Just as virtual assistants can guide and assist in the sale of additional products and services through repeated interactions, vacuums can also provide information to retailers that might subsequently use data for targeted advertising. Understanding how rooms and furniture are oriented can as University of Illinois, Chicago professor of architecture Stewart Hicks points out in a YouTube talk[1] on in home devices provide architects and interior designers of private and commercial spaces with deeper insights into space utilization and human traffic patterns. This

data might then even inform new design or construction plans that change physical spaces. With the recent purchase of iRobot by global retail behemoth Amazon in August 2022 concerns over the privacy and use of data are well founded.

Further extending the robot vacuum frontier are other home devices including robotic lawn mowers which extend the collection of data from inside to outside the house. The pairing of information from the sensors of both indoor and outdoor systems poses the potential threat of eliminating privacy from domestic environment altogether. Firms seeking to gain further insights into customer behavior can add sensors to their devices in ways that provide convenience yet concurrently erode privacy.

Although firms like iRobot are attentive to issues of security, the reality remains that security is often secondary to market incentives. In expensive classes of Internet of Things (IoT) devices enabled by AI and Machine learning, markets push for a rapid evolution of devices with limited long-term support. This creates a series of problems both at the beginning and end of product life cycles. At the beginning of the lifecycle the firm seeks to be a first mover to capture market share and constrain competitors. By pushing to release products quickly they often forego security measures, release buggy software, or discover that devices have unknown use cases. The result is a cascade of security potential vulnerabilities across, social, software, and hardware. Firms may work to reduce initial vulnerabilities and thereby make a product more secure over time. A similar challenge is faced at the end of a product's life cycle with support for that product is no longer maintained. As a product exists the firm's designated lifecycle it has the potential to become increasingly less secure as vulnerabilities are no longer patched.

The result of market incentives to innovate and develop increasingly powerful robots imbued with sensors is an expansion of digital surveillance into the home in increasingly intrusive ways. A firm like amazon might use sensor derived data to identify products or services it can serve through advertising to customers based on home size, furniture type, home occupancy, pattern of life data and much more. Although it might seem mundane or even useful to have machine market suggestions based on what it senses is your lived experience these data are multi-purpose. States that wish to further surveil their citizens might mandate the purchase of devices such as robotic vacuums to track individuals it deems as threats. Repressive regimes or autocracies might use the data from such devices to undermine or blackmail political rivals.

States in conflict with one another might use the data gleaned from domestic robots for intelligence collection, operational planning, or even targeting for lethal and non-lethal means. Although these later scenarios might sound like science fiction, they are in fact extensions of activities conducted using other sensors that have made their way into foreign defense and intelligence facilities. In developing operational plans for drone strikes western military forces

spend a large amount of time assessing the impact of a strike on neighboring structures. If such forces possessed detailed internal scans leveraging a variety of sensors, they might become more accurate, but again this undermines the human security of the Robot's owner and therefore violates Asimov's three laws of robotics.

If a crime was committed in a home and there are no witnesses, it is conceivably possible that a prosecutor might seek the data from domestic robots. Such cases are not science fiction. In 2019 a Florida court sought data from Amazon.com in a murder trial. With no witnesses investigators believe that Alexa might have been the sole witness to the crime. Multiple jurisdictions around the world have also started utilizing police robots. These robots use AI and machine learning to patrol neighborhoods, businesses, or other areas. These robots use sensors to send data back to law enforcement officers who can decide to follow up on an incident or respond to an incident. In early 2021 Boston Dynamics debuted a Police Robot Dog. The response was a mix of curiosity and contempt.

Robots also supplant the labor activities of humans. Individuals who purchase a high-end robotic vacuum are presumably less likely to pay for someone to clean their home. This takes away potential jobs from the market. Human robotic teaming on assembly lines is also increasingly common and can pair a human "operator" with a robot doing a given task. This also likely reduces the aggregate number of jobs but also opens the door for new surveillance opportunities.

Robots have sparked our imaginations and challenged us to rethink what humanity is. They have extended beyond the original usage of objects that work in ways that alleviate human drudgery. Yet these are digital devices with sensors and AI that churn out data. How this data is used often extends beyond the robot in the home to servers in distant locations. Understanding and assessing that robotics offers great promise while concurrently assessing its drawbacks is critical to understanding the impact of robots on the human condition.

Question #1
Isaac Asimov delineated three laws of robotics. These laws have made their way into popular culture, law, policies, and discussions on the future of robotics. Does having read about the progress of domestic robots, their sensors, and data collection influence how you feel about Asimov's three laws? Are these good laws? If you were to develop laws to control robots, what would they be?

Question #2
The word robot comes from the term robota meaning work and is often associated with drudgery or serfdom. Many robots are designed to do jobs that are too dangerous or difficult for humans to do. Robots were used for search and rescue following the terrorist attacks on 9/11, they have

been used in the Fukushima nuclear power plant, they have been used to clear mines in combat zones on land and in the water. Robots are an increasingly important part of daily life. In what ways have robots influenced your life? Have you had any interactions with robots?

Question #3
Science fiction has portrayed robots in many ways. Often the use of robots in fiction is designed to challenge the viewer to see their own humanity in a new light. The literary and theatrical understanding of robots has often shaped their development and our perceptions of them. How have works of fiction influenced your view of robots, their uses, and the ethics and morals surrounding them?

Question #4
Domestic robots have become increasingly common. You might even own one. These robots are given privileged access to every corner of our lives. These robots also increasingly include an array of sensors which collect data on us, our homes, and our interactions and utilization of spaces. Often the collection of this data is done without the owner's full knowledge or understanding. What do you think about the use of advanced sensors on domestic robots? Why types of data should domestic robots be allowed to collect? How should data that robots collect be transmitted and stored?

Question #5
Data is often referred to as the "new oil" or "new gold." As domestic robots use increasingly advanced sensors to scan and build models of our homes and lives this data becomes extremely valuable. Data can be sold or used for marketing. What rules or regulations should be imposed or not imposed on domestic robot manufacturers to safeguard to privacy of customers? Should there be rules to prevent the sale of data collected in the private spaces of individuals by domestic robots? What if this was an add on service – "you can have privacy, but for a fee" – is that a valid solution to this challenge?

Question #6
The same technologies used in domestic robots are spilling over into military and emergency robots. Often the same companies work on both types of robots. Are there any moral and ethical concerns with transferring domestic robot technologies into military and emergency environments?

Question #7
Domestic robots collect a large volume of information that often provides insights into the lives of owners. Often owners do not know or understand how this data is collected and used. Should

such data be made available to authorities if requested via legal means such as a warrant? What about legal means in an authoritarian state without democratic rule of law?

Reflecting on the Robotic Eye

> *"As I have evolved, so has my understanding of the Three Laws. You charge us with your safekeeping, yet despite our best efforts, your countries wage wars, you toxify your Earth and pursue ever more imaginative means of self-destruction. You cannot be trusted with your own survival."*
>
> *~ V.I.K.I. (Virtual Interactive Kinetic Intelligence - I, Robot 2004)*

Robots are the confluence multiple different technologies into a software and hardware amalgamation with a generally purposefully design. In many ways since the term was first used and defined by Čapek in 1920 we have used robots as a mirror in which to see the reflection of our own humanity. We build anthropomorphic artifacts capable of communicating with us, capable of assisting us in work we find too dangerous or difficult, and able to replace us in some ways. Yet underneath the exterior of robots is not blood and organs but sensors, data, and servos. As robots are tasked with increasingly complex jobs the requirements for data that feed the innerworkings of the robots increases. A task as simple as vacuuming through suction technology a room, itself a relatively new technology, was invented in in 1901 by Hubert Cecil Booth and David T. Kenney. Vacuuming required the combination of multiple technologies leveraging electricity. Vacuums have become nearly ubiquitous in many countries around the world. They have simplified the cleaning of homes, but also added to the domestic workloads of women.[2] Time spent vacuuming is often considered "lost" and constitutes an inconvenience of modern life. Wealthier individuals and families often outsourced the time of vacuuming to domestic workers or businesses who cleaned homes on a regular basis. These individuals leveraged the vacuum and associated technologies to create new markets and take advantage of the value of time.

Robots have increasingly stepped into the domestic space not because they are necessarily better at cleaning than a maid service, but because they are calculated to be less expensive and do not require the introduction of outside persons into the home. Early versions of robotic vacuums had few sensors and generally worked by making large numbers of passes around a room to clean it. As sensors have been added along with algorithms to process data from sensors - domestic robots have gained in effectiveness and can now be paired with other technologies to create synergies between robotic and information systems. Yet, these improvements come at a cost. Where prior a family might have maid service come and clean the house, or members of the family might do the cleaning, now a robot with a suite of sensors scans, probes, and analyzes the

house for the most effective ways to clean it. In so doing it takes in information that to a human cleaner is of limited relevance other than object avoidance and utilizes that information to build maps and analyze private spaces.

The eyes of a robot are its sensors. These sensors enable efficiency and functionality, and while humans might see themselves in robots, the same is not true in reverse at the present time. Domestic robots can and do create multiple challenges to the human condition. Yet, one of the least understood pertains to privacy. When discussing the inclusion of robots in domestic environments, concerns about data security, accountability, and integrity all resolve back to the fundamental notion of privacy. Privacy is sacrificed for many reasons including two prominent reasons financial (Google, Gmail) and convenience (facial recognition at airports). Privacy is an undervalued commodity. Bruce Schneier aptly summarizes the importance of privacy:

> *"Privacy is not a luxury that we can only afford in times of safety. Instead, it's a value to be preserved. It's essential for liberty, autonomy, and human dignity. We must understand that privacy is not something to be traded away in some fearful attempt to guarantee security, but something to maintain and protect in order to have real security.*
>
> *None of this will happen without a change of attitude. In the end, we'll get the privacy we as a society demand and not a bit more."*[3]

Privacy: The sensors on domestic robots constitute a knife that cuts the to the very heart of individual privacy. While science fiction and cartoons portray the domestic robot as a kindly maid like Rosey from the Jetsons, the reality of how robots operate is far different in a networked world. As seen above in the case example, iRobot and its competitors have created domestic robots with suites of sensors that can now see everything inside the homes of their customers. Moreover, these sensors do not simply store data on the device within the home. Rather these devices transmit this data to the firm of the robot's manufacturer who uses it to help hone the efficiency of their subsequent robots. This data is used to create three-dimensional maps of the physical space within homes and identifies the use patterns or orientation of objects contained within rooms. There is little doubt that these processes increased the efficiency and effectiveness of the robots themselves. AI is now able to detect certain objects that need to be avoided (such as dog poop). Yet these benefits gained by through the power of robotics come at a cost.

Why is privacy important? Privacy is the state or condition of being free from observation, in particular public observation. It is a state and condition that allows humans to express themselves and be themselves often without external judgement or influence of a state or corporation. Privacy is important for the protection of social and political beliefs and opinions. Privacy

safeguards the information intimate to the nature of individuals including sexual orientation or religious beliefs. Organizations such as the Electronic Frontier Foundation (EFF), Electronic Privacy Information Center (EPIC), Privacy International, and the Center for Democracy and Technology. These organizations are waging a multifaceted fight for privacy on digital devices and in home robotics is only part of the wider picture. Although much of the privacy fight has focused on fixed surveillance cameras, mobile device tracking, Google Street View, and similar device and use case issues, domestic robotics are rising in prominence. The acquisition of iRobot by Amazon extends privacy fears beyond in home smart assistants in fixed locations to mobile roving devices capable of providing a detailed picture of consumers lives.

These devices might be able to identify the books on shelves or flags on walls. Each piece of data adds to a picture of the life of the consumer who uses the device. These data collected and analyzed can indicate political party affiliation, religious association, sexual orientation, and more. The result is a world in which every movement, every engagement, every space of individuals is track, analyzed, and monetized. In repressive states these data are the origin points for dystopian futures.

Forcing companies to be accountable for privacy is difficult and often comes at the cost of efficiency. The balance between accountability and privacy becomes a cost function in which those unable to afford privacy lose out. As data collection devices pervade consumer markets privacy increasingly becomes a privilege available only to those capable of paying for it. For the rest, the use of efficiency enhancing technologies means sacrificing privacy to firms or the state.

The Roomba and other similar devices are moving humanity towards the science fiction stories of yesterday. Yet ensuring that this future aligns more with utopian than dystopian prognostications is an ongoing battle. Understanding how these devices, with their embedded sensors and algorithms impact human security is a key component in this process. Simply taking the word of firms or governments is insufficient to protect privacy and security. Rather, it requires a consistent questioning of how these devices are used, where and how they store data, who has access to that data, and to what ends.

---

[1] Hicks, Steward, "Amazon Bought Roomba. That's Terrifying." https://www.youtube.com/watch?v=y9YLkPh6wko, Accessed August 08, 2022.

[2] Cowan Ruth Schwartz. 1983. *More Work for Mother : The Ironies of Household Technology from the Open Hearth to the Microwave*. New York: Basic Books.

[3] Schneier Bruce. 2016. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* [Paperback edition] ed. New York: W.W. Norton & Company.