The dangers of trusting robots

Evan Selinger and Woodrow Hartzog, *BBC*, 12 August 2015

In February, a South Korean woman was sleeping on the floor when her robot vacuum ate her hair, forcing her to call for emergency help. It may not be the dystopian future that Stephen Hawking warned us about – where intelligent devices "spell the end of the human race" – but it does highlight one of the unexpected dangers of inviting robots into our home. There are many other examples of intelligent technology gone bad, but more often than not they involve deception rather than physical danger. Malevolent bots, designed by criminals, are now ubiquitous on social media sites and elsewhere online. The mobile dating app Tinder, for example, has been frequently infiltrated by bots posing as real people that attempt to manipulate users into using their webcams or disclosing credit card information. So it's not a stretch to imagine that untrustworthy bots may soon come to the physical world.

Meanwhile, increasing evidence suggests that we are susceptible to telling our deepest, darkest secrets to anthropomorphic robots whose cute faces may hide exploitative code – children particularly so. So how do we protect ourselves from double-crossing decepticons? Once you've invited a bot into your home, you need to manage your expectations. Movies and marketing may have primed us to expect sophisticated interaction with our robotic chums but we've still got a long way to go before they are as socially aware as they are often depicted. Given the gulf between expectation and reality, it's important to avoid being tricked by a fake-out known as a "Wizard-of-Oz setup", where users are led to believe that robots are acting autonomously when, in fact, human operators are remotely controlling some of their operations. Misjudging where behaviour originates can be an especially acute problem in cases where consumers feel so comfortable with a non-sentient device that they reveal intimate information that they would have withheld had they known a human was in the loop. Take the service "Invisible Boyfriend", for example. For a monthly subscription, romantic texts and voicemails are sent to your phone from a faux lover. Although the company initially sought to make the fake beau fully automated, the technology wasn't sophisticated enough, so in reality, human workers generate the amorous exchanges. But not all customers understand how the system works, and thanks to the hype surrounding artificial intelligence and well-documented cases of automated bots successfully tricking people into believing that they're real humans, some people might erroneously believe they're receiving computer-composed dialogue. The take-home message is clear: as robots become increasingly connected to the internet, and able to respond to natural language, you need to be especially vigilant about figuring out who or what you're talking to. We also need to think long and hard about how information is being stored and shared when it comes to robots that can record our every move. Some recording devices may have been designed for entertainment but can easily be adapted for more nefarious purposes. Take Nixie, the wearable camera that can fly off your wrist at a moment's notice and take aerial shots around you. It doesn't take much imagination to see how such technology could be abused.

Most people guard their secrets in the presence of a recording device. But what happens once we get used to a robot around the house, answering our every beck and call? We may be at risk of letting our guard down, treating them as extended members of the family. If the technology around us is able to record and process speech, images and movement – never mind eavesdrop on our juiciest secrets – what will happen to that information? Where will it be stored, who will have access? If our internet history is anything to go by, these details could be worth their weight in gold to advertising companies. If we grow accustomed to having trusted robots integrated into our daily lives, our words and deeds could easily become overly-exposed. So, what is the safest way to welcome robots into our homes, public spaces, and social lives? We should be cautiously optimistic that these intelligent machines could become enriching companions, while acknowledging that we need to determine strict boundaries for robots capable of deception and manipulation. We might think of expanding the reach of consumer protection agencies or creating new robotic-centric policies. Just as the advent of radio called for the formation of the Federal Radio Commission in the US, advances in robotics may call for the advent of a body responsible for the integration of robotics into society. Someone to turn to should your robot commit a crime, steal your credit card… or try to eat your hair.

Evan Selinger is an associate professor in the department of philosophy at the Rochester Institute of Technology. Woodrow Hartzog is an expert in privacy, media, and robotics law at Cumberland School of Law. This article draws from material in Hartzog's paper "Unfair and Deceptive Robots".

Location: http://www.bbc.com/future/story/20150812-how-to-tell-a-good-robot-from-the-bad